PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-177523
(43)Date of publication of application : 30.06.1998

(51)Int.Cl. G06F 12/14
G06F 12/00
G06F 12/00
G09C 1/00
H04L 9/14

(21)Application number : 08-335594
(22)Date of filing : 16.12.1996

(71)Applicant : MITSUBISHI ELECTRIC CORP
(72)Inventor : FUJII SEIJI

(54) MULTIMEDIA INFORMATION SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To guarantee the execution of multimedia information to the user of a multimedia information system based on the terms of the contract made by the user by eliminating unauthorized access to the multimedia information.
SOLUTION: A multimedia information server 6 is provided with a ciphering system deciding means 8a which decides an enciphering means which enciphers multimedia information and a decoding means which decodes enciphered multimedia information based on the terms of the contract made by a user stored in a user information database 9 and a transmitting means 7 which enciphers the multimedia information stored in the database 10 by using the enciphering means decided by the means 8a and transmits the enciphered multimedia information and a multimedia client 1 is provided with a receiving means 4 which decodes the enciphered multimedia information transmitted from the transmitting means 7 by using the decoding means decided by the deciding means 8.

CLAIMS

[Claim(s)]
[Claim 1]A multimedia information system provided with the following elements.
(a) The User Information memory measure which memorizes contract information with a user;

(b) A multimedia information memory measure which memorizes multimedia information containing a charactera figurea soundStill Picture Sub-Divisionor an animation;
(c) A server provided with the following elements;
(c1) A ciphering system deciding means which determines an encoding means which enciphers the above-mentioned multimedia informationand a decoding means which decodes multimedia information enciphered by this encoding means based on the above-mentioned contract information memorized by the above-mentioned User Information memory measure;
(c2) A transmitting means which enciphers multimedia information memorized by the above-mentioned multimedia information memory measure using an encoding means determined by this ciphering system deciding meansand transmits this enciphered multimedia information;
(d) A client which is provided with the following elements and requires transmission of the above-mentioned multimedia information of the above-mentioned server;
(d1) A reception means which decodes encryption multimedia information transmitted by the above-mentioned transmitting means using a decoding means determined by the above-mentioned ciphering system deciding means.
[Claim 2]Have a cipher system memory measure which memorizes two or more decoding means which decode data enciphered by two or more encoding means which perform encryption differentrespectivelyand each of this encoding meansand the above-mentioned serverAn encoding means and a decoding means which were determined by the above-mentioned ciphering system deciding means are taken out from the above-mentioned cipher system memory measureHave a cipher system transmitting means which transmits this taken-out encoding means and decoding meansand the above-mentioned transmitting meansThe multimedia information system according to claim 1 enciphering using an encoding means transmitted by the above-mentioned cipher system transmitting meansand decoding the above-mentioned reception means using a decoding means transmitted by the above-mentioned cipher system transmitting means.
[Claim 3]The above-mentioned transmitting means is provided with a cipher system memory measure which memorizes two or more encoding means which perform encryption differentrespectivelyTake out an encoding means determined by the above-mentioned ciphering system deciding means from the above-mentioned cipher system memory measureencipher using this taken-out encoding meansand the above-mentioned reception meansIt has a decode system memory measure which memorizes two or more decoding means which decode data enciphered by encoding means memorized by the above-mentioned cipher system memory measureThe multimedia information system according to claim 1 taking out a decoding means determined by the above-mentioned ciphering system deciding means from the above-mentioned decode system memory measureand decoding using this taken-out

decoding means.
[Claim 4]Have an area information memory measure which memorizes area information which shows an usable area of the above-mentioned encoding meansand the above-mentioned ciphering system deciding meansThe multimedia information system according to claim 1 characterized by determining the above-mentioned encoding means and the above-mentioned decoding means based on the above-mentioned area information memorized by the above-mentioned contract information memorized by the above-mentioned User Information memory measure and the above-mentioned area information memory measure.
[Claim 5]The multimedia information system comprising according to claim 1:
Two or more encryption execution means which perform an encoding means which enciphers multimedia information with which the above-mentioned ciphering system deciding means transmitted an encoding means and a decoding means which were newly determinedand the above-mentioned transmitting means was remembered to be by the above-mentioned multimedia information memory measure.
A cipher system alteration means which makes the above-mentioned encryption execution means which is not under execution perform the new encoding means transmitted by the above-mentioned ciphering system deciding means.
Two or more decoding execution means which perform a decoding means which decodes encryption multimedia information which was equipped with a transmission control means which transmits multimedia information enciphered by the above-mentioned encryption execution meansand to which the above-mentioned reception means was transmitted by the above-mentioned transmission control means.
A decode system alteration means which makes the above-mentioned decoding execution means which is not under execution perform the new decoding means transmitted by the above-mentioned ciphering system deciding means.

[Claim 6]The above-mentioned transmission control means builds send data which stored classification of an encoding means used in order to encipher as multimedia information enciphered by the above-mentioned encryption execution meansand transmitsThe above-mentioned decode system alteration means receives the above-mentioned send dataand distinguishes an encoding means which enciphered the above-mentioned multimedia information based on the above-mentioned classification stored in this received dataThe multimedia information system according to claim 5 making the above-mentioned decoding execution means perform a decoding means corresponding to this encoding means.
[Claim 7]A multimedia information system provided with the following elements.
(a) The User Information memory measure which memorizes contract information with a user;
(b) A multimedia information memory measure which memorizes multimedia information containing a charactera figurea soundStill Picture Sub-Divisionor an

animation;
(c) A server provided with the following elements;
(c1) A transmitting means which enciphers multimedia information memorized by the above-mentioned multimedia information memory measureand transmits this enciphered multimedia information;
(c2) Receive execution information of the above-mentioned multimedia informationand contract information memorized by this execution information and the above-mentioned User Information memory measure is comparedA control means which distinguishes whether the above-mentioned multimedia information is performed based on the above-mentioned contract informationand controls transmission of multimedia information by the above-mentioned transmitting means;
(d) A client which is provided with the following elements and requires transmission of the above-mentioned multimedia information of the above-mentioned server;
(d1) A reception means which decodes encryption multimedia information transmitted by the above-mentioned transmitting means;
(d2) An execution means which performs multimedia information decoded by this reception means;
(d3) An execution information transmitting means which transmits execution information which shows a state under execution of this execution means to the above-mentioned control means.
[Claim 8]The above-mentioned server is provided with an execution information transmission system determination means to determine a transmission system of the above-mentioned execution information by the above-mentioned execution information transmitting means based on contract information memorized by the above-mentioned User Information memory measureThe multimedia information system according to claim 7wherein the above-mentioned execution information transmitting means transmits the above-mentioned execution information with a transmission system determined by the above-mentioned execution information transmission system determination means.
[Claim 9]Memorize the above-mentioned User Information memory measureand contract information with a userand execution control information over multimedia information the above-mentioned control meansExecution information which received [above-mentioned] is compared with contract information and execution control information which were memorized by the above-mentioned User Information memory measureThe multimedia information system according to claim 7 distinguishing whether the above-mentioned multimedia information is performed based on the above-mentioned contract information and the above-mentioned execution control informationand controlling transmission of the above-mentioned multimedia information.
[Claim 10]Memorize the above-mentioned multimedia information memory measureand execution constraints which restrain execution of the above-mentioned

multimedia information and this multimedia information the above-mentioned control meansContract information memorized by the above-mentioned User Information memory measure in execution information which received [above-mentioned]And it compares with execution constraints memorized by the above-mentioned multimedia information memory measureThe multimedia information system according to claim 7 distinguishing whether the above-mentioned multimedia information is performed based on the above-mentioned contract information and the above-mentioned execution constraintsand controlling transmission of the above-mentioned multimedia information.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention]This invention relates to the multimedia information system which enciphers and provides the user who contracted with the multimedia information which consists of a charactera figurea soundStill Picture Sub-Divisionor an animation.

[0002]

[Description of the Prior Art]Drawing 20 is an outline block diagram showing the conventional multimedia information system shownfor example in JPH6-44122A. The multimedia information accumulating part which 50 enciphers the multimedia file which consists of various-media data of a charactera figurea soundStill Picture Sub-Divisionan animationetc.and is accumulated in a figureThe multimedia information Management Department which manages input and output of a multimedia file [as opposed to the multimedia information accumulating part 50 in 51]and 52 are output units which display the contents of the multimedia file.

[0003]Drawing 21 is a block diagram of the media data which is a component of the multimedia file accumulated in the multimedia information accumulating part 50. The enciphering key information for 60 responding to media dataand 60a responding to a user's security leveland distinguishing whether it is accessible data in a figureThe position and size information 60b indicates the display position and the size to display on a display screen to beThe media kind information 60c indicates the media classification of media data to beand 60 d are the output unit associated data which added the data of the data format different from the time of an input for the correspondence to the display screen from which presentation capability differs. Thusit has the enciphering key information for distinguishing whether access by a user is possible for every media dataand a security level can be changed by each media data unit which constitutes the multimedia file.

[0004]Nextoperation is explained. If a user makes demands on the multimedia

information Management Department 51 for the output of a multimedia filethe multimedia information Management Department 51 will take out the media data 60 which constitutes the multimedia file with an output request from the multimedia information accumulating part 50. Nextthe multimedia information Management Department 51 analyzes a user's security leveland distinguishes whether it is accessible media data with the user's security level based on the enciphering key information 60a included in each media data 60. And when a user distinguishes that it is accessible media dataonly this accessible media data 60 is set as the object of an outputand it changes into the data format according to the presentation capability of the output unit 52and outputs to the output unit 52.

[0005]

[Problem to be solved by the invention]The conventional multimedia information system is constituted as mentioned aboveaccumulated the enciphered multimedia informationand has transmitted to the user. Thereforesince the same cipher system will be used over a long period of timecommo data is intercepted by third parties other than the user who has contracted and the cipher system was decodedthere was a problem that a third party could access unjustly to the multimedia information transmitted to the user.

[0006]Before transmitting multimedia informationonly check conditions of contract about execution of a user's multimedia informationand during execution of multimedia informationSince it was not able to be confirmed whether a user is performing correctly based on conditions of contractthere was a problem that multimedia information will be able to be performed unjustly.

[0007]There was a problem that execution of multimedia information according to conditions of contract about execution of multimedia information of various userssuch as execution of multimedia information by time and a time basis and execution frequencywas uncontrollable.

[0008]This invention is made in order to cancel the above problemsand it eliminates unjust access to multimedia information by a third partyand an object of invention is to obtain a multimedia information system which guarantees that a user performs multimedia information based on conditions of contract.

[0009]

[Means for solving problem]The multimedia information system according to claim 1 is provided with the following elements.

(a) The User Information memory measure which memorizes contract information with a user;

(b) A multimedia information memory measure which memorizes multimedia information containing a charactera figurea soundStill Picture Sub-Divisionor an animation;

(c) A server provided with the following elements;

(c1) A ciphering system deciding means which determines an encoding means which

enciphers the above-mentioned multimedia informationand a decoding means which decodes multimedia information enciphered by this encoding means based on the above-mentioned contract information memorized by the above-mentioned User Information memory measure;
(c2) A transmitting means which enciphers multimedia information memorized by the above-mentioned multimedia information memory measure using an encoding means determined by this ciphering system deciding meansand transmits this enciphered multimedia information;
(d) A client which is provided with the following elements and requires transmission of the above-mentioned multimedia information of the above-mentioned server;
(d1) A reception means which decodes encryption multimedia information transmitted by the above-mentioned transmitting means using a decoding means determined by the above-mentioned ciphering system deciding means.
[0010]The multimedia information system according to claim 2Have a cipher system memory measure which memorizes two or more decoding means which decode data enciphered by two or more encoding means which perform encryption differentrespectivelyand each of this encoding meansand the above-mentioned serverAn encoding means and a decoding means which were determined by the above-mentioned ciphering system deciding means are taken out from the above-mentioned cipher system memory measureIt has a cipher system transmitting means which transmits this taken-out encoding means and decoding meansthe above-mentioned transmitting means is enciphered using an encoding means transmitted by the above-mentioned cipher system transmitting meansand the above-mentioned reception means is decoded using a decoding means transmitted by the above-mentioned cipher system transmitting means.
[0011]The multimedia information system according to claim 3It has a cipher system memory measure which memorizes two or more encoding means which perform encryption differentrespectivelyThe transmitting means which takes out the encoding means determined by the above-mentioned ciphering system deciding means from the above-mentioned cipher system memory measureand is enciphered using this taken-out encoding meansIt has a decode system memory measure which memorizes two or more decoding means which decode the data enciphered by the encoding means memorized by the above-mentioned cipher system memory measureThe decoding means determined by the above-mentioned ciphering system deciding means is taken out from the above-mentioned decode system memory measureand it has a reception means decoded using this taken-out decoding means.
[0012]The multimedia information system according to claim 4Have an area information memory measure which memorizes the area information which shows the usable area of the above-mentioned encoding meansand the above-mentioned ciphering system deciding meansBased on the above-mentioned area information memorized by the above-mentioned contract information memorized by the above-

mentioned User Information memory measure and the above-mentioned area information memory measurethe above-mentioned encoding means and the above-mentioned decoding means are determined.
[0013]The multimedia information system according to claim 5Have a ciphering system deciding means which transmits the newly determined encoding means and a decoding meansand the above-mentioned transmitting meansTwo or more encryption execution means which perform the encoding means which enciphers the multimedia information memorized by the above-mentioned multimedia information memory measureThe cipher system alteration means which makes the above-mentioned encryption execution means which is not under execution perform the new encoding means transmitted by the above-mentioned ciphering system deciding meansHave a transmission control means which transmits the multimedia information enciphered by the above-mentioned encryption execution meansand the above-mentioned reception meansIt has two or more decoding execution means which perform the decoding means which decodes the encryption multimedia information transmitted by the above-mentioned transmission control meansand a decode system alteration means which makes the above-mentioned decoding execution means which is not under execution perform the new decoding means transmitted by the above-mentioned ciphering system deciding means.
[0014]The multimedia information system according to claim 6A transmission control means which builds send data which stored classification of an encoding means used in order to encipher as multimedia information enciphered by the above-mentioned encryption execution meansand transmitsThe above-mentioned send data is receivedan encoding means which enciphered the above-mentioned multimedia information based on the above-mentioned classification stored in this received data is distinguishedand it has a decode system alteration means which makes the above-mentioned decoding execution means perform a decoding means corresponding to this encoding means.
[0015]The multimedia information system according to claim 7 is provided with the following elements.
(a) The User Information memory measure which memorizes contract information with a user;
(b) A multimedia information memory measure which memorizes multimedia information containing a charactera figurea soundStill Picture Sub-Divisionor an animation;
(c) A server provided with the following elements;
(c1) A transmitting means which enciphers multimedia information memorized by the above-mentioned multimedia information memory measureand transmits this enciphered multimedia information;
(c2) Receive execution information of the above-mentioned multimedia informationand contract information memorized by this execution information and the

above-mentioned User Information memory measure is comparedA control means which distinguishes whether the above-mentioned multimedia information is performed based on the above-mentioned contract informationand controls transmission of multimedia information by the above-mentioned transmitting means;
(d) Client which is provided with the following elements and requires transmission of the above-mentioned multimedia information of the above-mentioned server;
(d1) Reception means which decodes the encryption multimedia information transmitted by the above-mentioned transmitting means;
(d2) Execution means which performs multimedia information decoded by this reception means;
(d3) The execution information transmitting means which transmits the execution information which shows the state under execution of this execution means to the above-mentioned control means.
[0016]The multimedia information system according to claim 8The above-mentioned server is equipped with an execution information transmission system determination means to determine the transmission system of the above-mentioned execution information by the above-mentioned execution information transmitting means based on the contract information memorized by the above-mentioned User Information memory measureThe above-mentioned execution information transmitting means transmits the above-mentioned execution information with the transmission system determined by the above-mentioned execution information transmission system determination means.
[0017]The multimedia information system according to claim 9The User Information memory measure which memorizes contract information with a userand the execution control information over multimedia informationThe execution information which received [above-mentioned] is compared with the contract information and the execution control information which were memorized by the above-mentioned User Information memory measureIt distinguishes whether the above-mentioned multimedia information is performed based on the above-mentioned contract information and the above-mentioned execution control informationand has a control means which controls transmission of the above-mentioned multimedia information.
[0018]The multimedia information system according to claim 10A multimedia information memory measure which memorizes execution constraints which restrain execution of the above-mentioned multimedia information and this multimedia informationContract information memorized by the above-mentioned User Information memory measure in execution information which received [above-mentioned]And it compares with execution constraints memorized by the above-mentioned multimedia information memory measuredistinguishes whether the above-mentioned multimedia information is performed based on the above-mentioned contract information and the above-mentioned execution constraintsand has a control means which controls transmission of the above-mentioned multimedia information.

[0019]
[Mode for carrying out the invention]
Below embodiment 1. explains this inventionreferring to a figure based on an embodiment. Drawing 1 is a block diagram of a multimedia information system of Embodiment 1. In a figurewhile a multimedia client as which 1 requires transmission of multimedia informationand 2 receive a demand from a userAn input output means which outputs an executed result of multimedia informationand 3 perform multimedia informationAn execution control means to transmit an executed result to the input output means 2and 4 receive and decode enciphered multimedia informationA network and 6 a reception means which transmits to the execution control means 3and 5 A multimedia information serverWhile a transmitting means which 7 enciphers multimedia information and transmits to the multimedia client 1 via the network 5and 8 determine a cipher systemA user information data base as an information control means which controls transmission of multimedia informationand a User Information memory measure which is accumulating contract information of all the users who have made a contract of 9A multimedia information database as a multimedia information memory measure for which 10 is accumulating all the multimedia information for which the multimedia information server 6 provides service11 is a cipher system database as a cipher system memory measure which is accumulating a key generating meansan encoding meansand a decoding means of all the cipher systems which can be used by the multimedia information server 6.
[0020]The information control means 8 comprises the ciphering system deciding means 8athe cipher system transmitting means 8band the key generation part 8c. The ciphering system deciding means 8a determines a cipher system used when transmitting multimedia information based on a user's contract information accumulated in the user information data base 9. The cipher system transmitting means 8b takes out a key generating meansan encoding meansand a decoding means of a cipher system determined by the ciphering system deciding means 8a from the cipher system database 11a key generating means transmits to the key generation part 8can encoding means transmits to the transmitting means 7and a decoding means transmits it to the reception means 4. The key generation part 8c generates an enciphering key and a decode key using a key generating means transmitted by the cipher system transmitting means 8b.
[0021]As illustratedthis system the multimedia information server 6 and two or more multimedia clients 1It is connected to the network 5and the multimedia information server 6 takes out multimedia information demanded from the multimedia client 1 from the multimedia information database 10enciphersand transmits to the multimedia client 1.
[0022]Drawing 2 is a block diagram showing composition of contract information accumulated in the user information data base 9. As for a contract information record with a userand 9bin a figure9a is [a user's address and 9e of a user registration

number and 9c (a user's name and 9 d)] a contract type with a user. The contract type 9e is the information for determining a cipher system.
[0023]Drawing 3 is a block diagram showing composition of multimedia information accumulated in the multimedia information database 10. In a figurea real whereabouts type number which a multimedia information number to identify 10a on a multimedia information recordand for 10b identify multimedia information uniquely and 10c show a name of multimedia informationand shows 10 d of execution means of multimedia informationand 10 f are multimedia information.
[0024]Drawing 4 is a block diagram showing composition of a cipher system accumulated in the cipher system database 11. A cipher system number to identify 11a on a cipher system recordand for 11b identify a cipher system uniquely in a figureA key generating means which 11c generates a name of a cipher system and generates 11 d of enciphering keys and decode keysan encoding means as which 11e enciphers multimedia informationand 11 f are decoding means which decode enciphered multimedia information.
[0025]Nextit explains based on the flow chart of ****** of operation and drawing 5. Out of the multimedia information number 10a and the multimedia information name 10c which are displayed on the input output means 2. When a user chooses the one multimedia information number 10a (Step S1)the execution control means 3The user registration number 9b inputted by the user and the selected multimedia information number 10a are transmitted to the cipher system transmitting means 8b of the multimedia information server 6 (Step S2). The cipher system transmitting means 8b outputs the user registration number 9b to the ciphering system deciding means 8a (Step S3).
[0026]The ciphering system deciding means 8a acquires a user's contract information record 9a from the user information data base 9 by making the user registration number 9b into a search condition (step S4)The cipher system number 11b of the cipher system which determined and determined the cipher system based on the contract type 9e in the acquired contract information record 9a is outputted to the cipher system transmitting means 8b (Step S5).
[0027]The cipher system transmitting means 8b acquires the key generating means 11dthe encoding means 11eand the decoding means 11f from the cipher system database 11 by making the cipher system number 11b into a search condition (Step S6). The cipher system transmitting means 8b outputs the key generating means 11d to the key generation part 8c (Step S7)and the key generation part 8c uses this outputted key generating means 11dand generates an enciphering key and a decode keyand it outputs it to the cipher system transmitting means 8b (Step S8). The enciphering key with which the cipher system transmitting means 8b was generated by the key generation part 8cThe encoding means 11e acquired from the cipher system database 11 is outputted to the transmitting means 7 (step S9)and the decode key generated by the key generation part 8c and the decoding means 11f

acquired from the cipher system database 11 are transmitted to the reception means 4 (Step S10).

[0028]Nextthe cipher system transmitting means 8b makes a search condition the multimedia information number 10a transmitted at Step S2 and10 f of multimedia information which the user chose is taken out from the multimedia information database 10and it divides into a blockand outputs to the transmitting means 7 (Step S11). Using the enciphering key and the encoding means 11e which were outputted by step S9the transmitting means 7 enciphers each block of 10 f of multimedia informationand transmits to the reception means 4 (Step S12).

[0029]The reception means 4 decodes each block of 10 f of received encryption multimedia information using a decode key and the decoding means 11f to which it was transmitted at Step S10and transmits to the execution control means 3 (Step S13). The execution control means 3 performs 10 f of decoded multimedia informationand outputs an executed result to the input output means 2 (Step S14).

[0030]As mentioned abovesince according to this embodiment a cipher system was chosen based on a user's contract type and a cipher system is changed for every user out of a cipher system of a large number accumulated in the cipher system database 11Since a guess of a cipher system is difficult for a third partyit is effective in the ability to eliminate unjust access.

[0031]Although the ciphering system deciding means 8a determined a cipher system and a form to which the cipher system transmitting means 8b transmits a key generating meansan encoding meansand a decoding means was shown by this embodimentIt can also constitute so that the ciphering system deciding means 8a may have a function of the cipher system transmitting means 8b and may transmit each means corresponding to a determined cipher system.

[0032]When neither an encoding means performed by the embodiment 2. transmitting means 7 nor a decoding means performed by the reception means 4 can be changedAs shown in drawing 6a multimedia information system is also realizable from the information control means 8 changing the transmitting means 7and ordering and changing using several different transmitting means 7 and reception means 4 of a cipher systemso that the reception means 4 of the same cipher system may be used to the execution control means 3.

[0033]When transmitting the decoding means 11f via embodiment 3. and a networkin order to shorten that the decoding means 11f may be stolen by the third party and time to transmit the decoding means 11f to the reception means 4As shown in drawing 7the decoding means database 12 which accumulated only the decoding means in the multimedia client side can also be distributed and arranged.

[0034]In an embodiment 4. panas shown in drawing 8it can also constitute so that the transmitting means 7 by the side of a multimedia information server may have the encoding means database 13 and the reception means 4 of a multimedia client side may have the decoding means database 12 in an inside.

[0035]According to the embodiment 5. embodiment 1although the cipher system was determined based on the contract type in contract information with a userwhen two or more candidates of the cipher system corresponding to a contract type remainin order to determine a cipher system as oneinformation other than a contract type is needed.
[0036]When transmitting and receiving the data enciphered between the user and the multimedia information serveran usable cipher system may be restricted by the law of an inhabitable area. Since the same cipher system cannot necessarily be used at all in the area where a multimedia client exists with an usable cipher system and a cipher system usable in the area where a multimedia information server existsit is necessary to determine the cipher system which can be used at both places butand. This cannot be judged only by conditions of contract with a user individual. Soa cipher system database is made into the structure shown in drawing 9 in this embodiment. The cipher system database shown in drawing 9 adds 11 g of usable area information which shows the usable area of each cipher system to the cipher system database shown in drawing 4.
[0037]Although the composition of the multimedia information system of this embodiment is the same as the composition of drawing 1 explained by Embodiment 1operation of the cipher system determination in the ciphering system deciding means 8a differs from the thing of Embodiment 1. Different operations are step S4 explained by Embodiment 1and S5. Different operation is explained below. According to this embodimentthe ciphering system deciding means 8a acquires a user's contract information record 9a from the user information data base 9 by making the user registration number 9b into a search condition. Nextthe cipher system record 11a is picked out from the cipher system database 11 shown in drawing 8. And 9 d of addresses in the acquired contract information record 9a investigate whether it agrees in 11 g of usable area information in the cipher system record 11a. When the agreeing cipher system is pluralitythe cipher system which agrees from the inside in the contract type 9e in a user's contract information record 9a is determinedand the cipher system number 11b of the determined cipher system is outputted to the cipher system transmitting means 8b.
[0038]As mentioned abovea cipher system can be chosen also when the cipher system which can be used changes with areassince a cipher system is determined based on a user's contract type and the usable area information of a cipher system according to this embodiment.
[0039]Embodiment 6. drawing 10 is a block diagram of the multimedia information system of Embodiment 6. In a figurethe execution control means 3 and the reception means 4 constitute a multimedia client like what was shown in drawing 1and the transmitting means 7 and the information control means 8 constitute a multimedia information server like what was shown in drawing 1.
[0040]In the information control means 8the ciphering system deciding means 8aWhen

a cipher system is changednewly determine a cipher system and the cipher system transmitting means 8bTaking out a key generating meansan encoding meansand a decoding means from the cipher system database 11 shown in drawing 1 based on a new cipher systema key generating means transmits to the key generation part 8can encoding means transmits to the transmitting means 7and a decoding means transmits to the reception means 4. The transmitting means 7 comprises the cipher system alteration means 7athe encryption execution means 7b and 7cand the transmission control means 7d. The cipher system alteration means 7a changes the encryption execution means 7b and 7c used by the transmitting means 7 based on the new encoding means transmitted by the cipher system transmitting means 8b. The encryption execution means 7b and 7c perform the encoding means transmitted from the cipher system transmitting means 8bencipher the data outputted from the transmission control means 7dand output the result to the transmission control means 7d. The transmission control means 7d outputs the block of the multimedia information outputted from the information control means 8 to the encryption execution means 7b or 7cand transmits the multimedia information enciphered by the encryption execution means 7b and 7c to the reception means 4.

[0041]The reception means 4 comprises the decode system alteration means 4athe decoding execution means 4b and 4cand the reception control means 4d. The decode system alteration means 4a changes the decoding execution means 4b and 4c used by the reception means 4 based on the new decoding means transmitted by the cipher system transmitting means 8b. The decoding execution means 4b and 4c perform the decoding means transmitted from the cipher system transmitting means 8bdecode the data outputted from the reception control means 4dand output the result to the reception control means 4d. The reception control means 4d outputs the encryption multimedia information outputted from the transmission control means 7d to the decoding execution means 4b or 4cand transmits the multimedia information decoded by the decoding execution means 4b and 4c to the execution control means 3.

[0042]Nextoperation is explained based on the flow chart of drawing 11. The cipher system transmitting means 8b transmits the enciphering key and encoding means which were determined by the ciphering system deciding means 8a to the cipher system alteration means 7a (Step S20). The cipher system alteration means 7a outputs the enciphering key and encoding means which were received to the encryption execution means 7band sets them up encipher using the encryption execution means 7b (Step S21). The cipher system transmitting means 8b transmits to the decode system alteration means 4a of a decode key and the decoding means reception means 4 (Step S22). The decode system alteration means 4a outputs the decode key and decoding means which were received to the decoding execution means 4band sets them up decode using the decoding execution means 4b (Step S23).

[0043]The information control means 8 divides multimedia information into a blockand

transmits a block to the transmission control means 7d (Step S24). The transmission control means 7d outputs the received block to the encryption execution means 7b (Step S25). The encryption execution means 7b enciphers a block using the enciphering key and encoding means which were outputted at Step S21and outputs it to the transmission control means 7d (Step S26). The transmission control means 7d transmits the enciphered block to the reception control means 4d via the network 5 (Step S27).

[0044]The reception control means 4d will be outputted to the decoding execution means 4bif the block of the multimedia information enciphered from the network 5 is received (Step S28). The decoding execution means 4b decodes an encryption block using the decode key and decoding means which were outputted at Step S23and outputs it to the reception control means 4d (Step S29). The reception control means 4d transmits the decoded block to the execution control means 3 (Step S30).

[0045]Nextthe operation in the case of changing a cipher system is explained based on the flow chart of drawing 12 during execution of multimedia information. The information control means 8 will suspend transmission to the transmission control means 7d of a block of multimedia informationif the cipher system used now is changed (Step S40). The cipher system transmitting means 8b transmits the enciphering key and encoding means after change for which it opted by the ciphering system deciding means 8a to the cipher system alteration means 7a (Step S41). The cipher system alteration means 7a outputs the enciphering key and encoding means which were received to the encryption execution means 7cand the block received next is set up encipher using the encryption execution means 7c (Step S42). The cipher system transmitting means 8b transmits the decode key and decoding means after change for which it opted by the ciphering system deciding means 8a to the decode system alteration means 4a (Step S43). The decode system alteration means 4a outputs the decode key and decoding means which were received to the decoding execution means 4cand the encryption block received next is set up decode using the decoding execution means 4c (Step S44).

[0046]The information control means 8 cancels a stop of transmissiondivides multimedia information into a blockand resumes transmission of a block to the transmission control means 7d (Step S45). The transmission control means 7d outputs a received block to the encryption execution means 7c (Step S46). The encryption execution means 7c enciphers ****** and a blockand outputs an enciphering key and an encoding means after change outputted at Step S42 to the transmission control means 7d (Step S47). The transmission control means 7d transmits an enciphered block to the reception control means 4d via the network 5 (Step S48).

[0047]The reception control means 4d will be outputted to the decoding execution means 4cif a block of multimedia information enciphered from the network 5 is received (Step S49). A decode key and a decoding means which were outputted at

Step S42 are used for the decoding execution means 4cit decodes a blockand outputs it to the reception control means 4d (Step S50). The reception control means 4d transmits a decoded block to the execution control means 3 (Step S51).

[0048]As mentioned abovesince a cipher system to be used can be changed dynamically according to this embodimentwhen adding a cipher system to a multimedia information serverit is effective in that there is no necessity of changing hardware which constitutes a system.

[0049]Although the ciphering system deciding means 8a determined a new cipher system and the cipher system transmitting means 8b showed the form which transmits a key generating meansan encoding meansand a decoding means by this embodiment based on a new cipher systemThe ciphering system deciding means 8a has a function of the cipher system transmitting means 8band it can also constitute so that each means corresponding to a new cipher system may be transmitted.

[0050]In this embodimentas shown in drawing 10the encryption execution means 7b and 7c within the transmitting means 7 and the decoding execution means 4b and 4c within the reception means 4 may be not only two but two or more. When the cipher system used once is saved at the encryption execution means 7b and 7c and the decoding execution means 4b and 4c and the same cipher system is used againA new enciphering key is outputted to the encryption execution means 7b and 7ca new decode key is outputted to the decoding execution means 4b and 4cand the reuse of the encryption execution means 7bthe encoding means in 7cand the decoding execution means 4b and the decoding means in 4c is carried out.

[0051]When the encryption execution means 7b and 7c or the decoding execution means 4b and 4c are already in use and there is nothing intactit controls to use the low encryption execution means 7b and 7c or the decoding execution means 4b and 4c of frequency in use.

[0052]The embodiment 7. embodiment 7 creates the send data 14 constituted by the block of the enciphered multimedia information 14band the cipher system number 14a of the cipher system used for the encryptionas shown in drawing 13. Although the composition of a system is the same as that of the thing of drawing 10 explained by Embodiment 6processings of the transmission control means 7d and the reception control means 4d differ. The reception control means 4d which the transmission control means 7d created the send data shown in drawing 13transmitted to the reception control means 4d via the network 5and received thisThe cipher system number 14a determines the decoding means which decodes the enciphered multimedia information 14band either the decoding execution means 4b or the decoding execution means 4c is made to perform decoding.

[0053]Embodiment 8. drawing 14 is a block diagram of the multimedia information system of Embodiment 8. In a figure15 is a real whereabouts type database which is accumulating two or more means for performing multimedia information with the real whereabouts type number. The user information data base 9 is shown in drawing 2and

shows drawing 3 the multimedia information database 10. The execution control means 3 comprises the execution information control means 3a and the execution means 3b. The execution means 3b performs multimedia information decoded by the reception means 4and transmits an executed result to the input output means 2. The execution information control means 3a is a certain time intervaland transmits execution information when performing multimedia informationand a user's demand outputted by the input output means 2 to the multimedia information server 6. The accumulated time of execution of the user registration number 9bthe multimedia information number 10b under executionand the multimedia information by the present is included in execution information. The information control means 8 comprises the control means 8d and the multimedia information transmitting means 8e. The control means 8d receives the execution information of the multimedia information transmitted by the execution information control means 3aanalyzes the informationand controls the multimedia information transmitting means 8e. The multimedia information transmitting means 8e acquires multimedia information from the multimedia information database 10and transmits to the transmitting means 7. The transmitting means 7 enciphers multimedia information and transmits to the reception means 4.

[0054]Nextoperation until it starts execution of multimedia information is explained based on the flow chart of drawing 15. If a user chooses one multimedia informationthe execution information control means 3a will transmit the user registration number 9b and the multimedia information number 10b to the control means 8d (Step S60). The control means 8d picks out a user's contract information record 9a from the user information data base 9 by making the user registration number 9b into a search conditionIt is judged whether execution can be started at the time which could perform multimedia information with a demand from the contract type 9eor the demand suited (Step S61). If the control means 8d judges with the execution start of multimedia information being possibleit will pick out the multimedia information record 10a from the multimedia information database 10 by making the multimedia information number 10b into a search conditionand will acquire 10 d of real whereabouts type numbers (Step S62). Nextthe control means 8d takes out an execution means from the real whereabouts type database 15 by making 10 d of real whereabouts type numbers into a search conditionand transmits to the execution information control means 3a (Step S63). The execution information control means 3a outputs the received execution means to the execution means 3b (Step S64). The control means 8d outputs the multimedia information number 10b to the multimedia information transmitting means 8e (Step S65). The multimedia information transmitting means 8e picks out the multimedia information record 10a from the multimedia information database 10 by making the multimedia information number 10b into a search conditiondivides it into a blockand transmits to the transmitting means 7 (Step S66).

[0055]The transmitting means 7 enciphers a received block and transmits to the reception means 4 via the network 5 (Step S67). The reception means 4 decodes a received block and transmits to the execution means 3b (Step S68). The execution means 3b outputs a message which execution preparation ended to the input output means 2 (Step S69). A user inputs an execution start of multimedia information from the input means 2 (Step S70). If directions of an execution start are receivedthe execution information control means 3a will transmit a message of a start of execution of multimedia information to the control means 8dand will start calculation of accumulated time of execution (Step S71). The control means 8d will output a transmission start message to the multimedia information transmitting means 8eif a message of a start of execution of multimedia information is received (Step S72).
[0056]Nextoperation under execution of multimedia information is explained based on a flow chart of drawing 16. The multimedia information transmitting means 8e takes out multimedia information from the multimedia information database 10 by making the multimedia information number 10b into a search conditiondivides it into a blockand transmits to the transmitting means 7 (Step S80). The control means 8d starts calculation of accumulated time of execution of multimedia informationand waits for reception of execution information (Step S81). The transmitting means 7 enciphers a block of multimedia informationand transmits to the reception means 4 via the network 5 (Step S82). The reception means 4 decodes a received block and transmits to the execution means 3b (Step S83). If multimedia information is received from the reception means 4the execution means 3b will perform multimedia informationand will output an executed result to the input output means 2 (Step S84).
[0057]If fixed time passes when having repeated operation of Steps S80-S84 (Step S85)the execution information control means 3a will transmit the execution information which set the accumulated time of execution of the multimedia information by the present to the control means 8d (Step S86). The control means 8d calculates the absolute value of the difference of the accumulated time of the execution which the control means 8d calculatedand the accumulated time set to execution informationIt is confirmed whether the absolute value of the difference is over the range of the error which the control means 8d holds (Step S87)When having exceededit judges that the unjust execution which is not in agreement with (Step S88) and the contract type 9e was detectedand the message which shows the stop of transmission is outputted to the multimedia information transmitting means 8e (Step S88). The multimedia information transmitting means 8e stops transmission of multimedia information (Step S89).
[0058]As mentioned abovesince according to this embodiment transmission is suspended when the execution accumulated time of multimedia information is checked based on a contract type and it is over predetermined timeThe effect of preventing execution of the unjust multimedia information which breaks conditions of contract is during execution of multimedia information.

[0059]Embodiment 9. drawing 17 is a block diagram of a multimedia information system of Embodiment 9. In a figure8 f is an execution information transmission system determination means to determine timing which transmits execution information from the execution information control means 3a by demand from the control means 8d.
[0060]Nextoperation is explained. If a user chooses one multimedia informationthe execution information control means 3a will transmit the user registration number 9b and the multimedia information number 10b to the control means 8d. The control means 8d picks out a user's contract information record 9a by making the user registration number 9b into a search condition from the user information data base 9and outputs the contract type 9e to the execution information transmission system determination means 8f. The execution information transmission system determination means 8f has a list of number of an execution information transmission system which can be used by the execution information control means 3a in an insideand outputs a system number of a system which chose and chose one in a list from the contract type 9e to the control means 8d. The control means 8d transmits a system number to the execution information control means 3a. The execution information control means 3a will transmit execution information to the control means 8d based on an execution information transmission system of a system numberif a system number is received.
[0061]The transmission system of execution information has a system system which transmits execution informationa system which transmits execution information with a certain fixed time intervalor a system which transmits execution information with an irregular time intervalonly when a user's demand is during information execution.
[0062]As mentioned abovesince a user and a third party intercept at time to send execution information by changing the system which transmits execution information to a multimedia information server and it becomes impossible to transmit the execution information of ** according to this embodimentIt is effective in preventing execution of unjust multimedia information.
[0063]As opposed to the user information data base which embodiment 10. drawing 18 is a block diagram of the user information data base in Embodiment 10and was shown in drawing 2The multimedia information numbers 9f and 9h and the multimedia execution control information 9g and 9i are addedand the number and execution control information on multimedia information that the user has made a contract of service are held. The system configuration of this embodiment is the same as that of what was shown in drawing 14.
[0064]Nextoperation is explained. If a user chooses one multimedia informationthe execution information control means 3a will transmit the user registration number 9b and the multimedia information number 10b to the control means 8d. The control means 8d picks out a user's contract information record 9a by making the user registration number 9b into a search condition from the user information data base 9and checks whether the multimedia information number 10b which the user is

demanding of the multimedia information numbers 9f and 9h in it is included. The control means 8d will judge whether the start of execution of multimedia information is possible based on the multimedia execution control information 9g and 9i corresponding to the multimedia information numbers 9f and 9hif the number which the user is demanding is found. When there is no number which the user is demandingit is judged whether the start of execution is possible at the time which had [whether multimedia information with a demand can be performed based on the contract type 9eand] the demand again.

[0065]If a user's control request occurs during execution of multimedia informationthe execution information control means 3a will transmit to the control means 8d by making the demand into execution information. It is judged whether based on the multimedia execution control information 9g and 9ithis demand can perform the control means 8d. If judged with it being possiblethe message which can be performed to the execution information control means 3a will be transmitted. The execution information control means 3a controls the execution means 3b based on a user's demand. If judged with it being impossiblea message [that it cannot perform to the execution information control means 3a] will be transmitted. The execution information control means 3a outputs a canceling [a user's demand] **** message to the input/output device 1.

[0066]As mentioned aboveaccording to this embodimentthe execution control information on the multimedia information which the user has made a contract of is stored in a user information data baseSince it distinguishes whether multimedia information is performed based on this execution control information and transmission of multimedia information is controlledit is effective in preventing execution of the unjust multimedia information which breaks conditions of contract.

[0067]Embodiment 11. drawing 19 is a block diagram of the multimedia information database in Embodiment 11and has added the execution constraints 10e which restrain execution of multimedia information to the multimedia information database shown in drawing 3. The system configuration of this embodiment is the same as that of what was shown in drawing 14.

[0068]Nextoperation is explained. If a user chooses one multimedia informationthe execution information control means 3a will transmit the user registration number 9b and the multimedia information number 10b to the control means 8d. The control means 8d picks out the contract type 9e of a user in a user's contract information record 9a from the user information data base 9 by making the user registration number 9b into a search condition. The control means 8d takes out the execution constraints 10e in the multimedia information record 10a from the multimedia information database 10 by making the multimedia information number 10b into a search conditionand checks whether a user's contract type 9e is included in the execution constraints 10e. When containedit is judged whether a start of execution is possible at time which a demand suited [whether multimedia information with a

demand can be performed from the contract type 9eand] again. When not containeda message which shows that a demand from a user was canceled and a demand from a user was canceled is transmitted to the execution information control means 3a. The execution information control means 3a outputs a canceling [a user's demand] **** message to the input/output device 1.

[0069]As mentioned aboveaccording to this embodimentexecution constraints for performing multimedia information are stored in a multimedia information databaseSince it distinguishes whether multimedia information is performed based on these execution constraints and transmission of multimedia information is controlledit is effective in preventing execution of unjust multimedia information which breaks conditions of contract.

[0070]

[Effect of the Invention]As mentioned abovethe encoding means which enciphers the invention ****** according to claim 1 and multimedia informationSince the cipher system is changed for every user by determining the decoding means which decodes the multimedia information enciphered by this encoding means based on contract information with a userSince the guess of a cipher system is difficult for a third partyit is effective in the ability to eliminate unjust access to multimedia information.

[0071]By according to the invention according to claim 2having a cipher system memory measure which memorizes two or more encoding means and two or more decoding meansand determining an encoding means and a decoding means based on contract information with a userSince the cipher system is changed for every userand the guess of a cipher system is difficult for a third partyit is effective in the ability to eliminate unjust access to multimedia information.

[0072]According to the invention according to claim 3the transmitting means which transmits encryption multimedia informationThe reception means which is provided with the cipher system memory measure which memorizes two or more encoding meansand decodes encryption multimedia informationSince it had the decode system memory measure which memorizes two or more decoding meansin order that there may be no necessity of transmitting a decoding means to a client from a serverit is effective in the ability to shorten a part for the air time of a decoding means.

[0073]Since according to the invention according to claim 4 it has an area information memory measure which memorizes the area information which shows the usable area of an encoding means and an encoding means and a decoding means are determined based on contract information and area information with a userAlso when the cipher system which can be used changes with areasit is effective in the ability to choose a cipher system.

[0074]According to the invention according to claim 5the transmitting means of a serverEquip the encryption execution means which is not under execution with the cipher system alteration means which performs encryptionand the reception means of a clientSince the cipher system used by having equipped the decoding execution

means which is not under execution with the decode system alteration means which performs decoding can be changed dynamicallywhen adding a cipher systemit is effective in that there is no necessity of changing the hardware which constitutes a system.

[0075]According to the invention according to claim 6since a cipher system can be known from send data by storing the classification of the encoding means used into the send data of encryption multimedia informationthere is no necessity of notifying a cipher system to a clientand it is effective in the ability to shorten time.

[0076]Since it distinguishes whether the execution information which shows the run state of the multimedia information in a client side is compared with contract information with a userand multimedia information is performed based on a contract according to the invention according to claim 7It is effective in preventing execution of the unjust multimedia information which breaks conditions of contract.

[0077]Since it intercepts at time to send execution information by determining the execution information transmission system from a client to a server based on contract information with a user and it becomes impossible to transmit the execution information of ** according to the invention according to claim 8It is effective in preventing execution of the unjust multimedia information which breaks conditions of contract.

[0078]According to the invention according to claim 9the execution control information on the multimedia information which the user has made a contract of is stored in the User Information memory measureSince it distinguishes whether multimedia information is performed based on this execution control information and transmission of multimedia information is controlledit is effective in preventing execution of the unjust multimedia information which breaks conditions of contract.

[0079]According to the invention according to claim 10the execution constraints which restrain execution of multimedia information are stored in a multimedia information memory measureSince it distinguishes whether multimedia information is performed based on these execution constraints and transmission of multimedia information is controlledit is effective in preventing execution of the unjust multimedia information which breaks conditions of contract.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1]It is a block diagram of the multimedia information system of Embodiment 1.

[Drawing 2]It is a block diagram of a user information data base.

[Drawing 3]It is a block diagram of a multimedia information database.

[Drawing 4]It is a block diagram of a cipher system database.

[Drawing 5]It is a flow chart which shows operation of the multimedia information system of Embodiment 1.
[Drawing 6]It is a block diagram of the multimedia information system of Embodiment 2.
[Drawing 7]It is a block diagram of the multimedia information system of Embodiment 3.
[Drawing 8]It is a block diagram of the multimedia information system of Embodiment 4.
[Drawing 9]It is a block diagram of the cipher system database of Embodiment 5.
[Drawing 10]It is a block diagram of the multimedia information system of Embodiment 6.
[Drawing 11]It is a flow chart which shows operation of the multimedia information system of Embodiment 6.
[Drawing 12]It is a flow chart which shows the operation in the case of changing the cipher system in the multimedia information system of Embodiment 6.
[Drawing 13]It is a block diagram of the send data of the multimedia information server in Embodiment 7.
[Drawing 14]It is a block diagram of the multimedia information system of Embodiment 8.
[Drawing 15]It is a flow chart which shows operation of the multimedia information system of Embodiment 8.
[Drawing 16]It is a flow chart which shows the operation under multimedia information execution in the multimedia information system of Embodiment 8.
[Drawing 17]It is a block diagram of the multimedia information system of Embodiment 9.
[Drawing 18]It is a block diagram of the user information data base in Embodiment 10.
[Drawing 19]It is a block diagram of the multimedia information database in Embodiment 11.
[Drawing 20]It is an outline block diagram of the conventional multimedia information system.
[Drawing 21]It is a block diagram of the media data in the conventional multimedia information system.
[Explanations of letters or numerals]
1 A multimedia client and 2 An input output means and 3 Execution control means3a An execution information control means and 3b An execution means and 4 A reception means and 4a Decode system alteration means4b and 4c A decoding execution means and 4 d A reception control means and 5 Network6 multimedia-information server and 7 A transmitting means and 7a Cipher system alteration means7b and 7c An encryption execution means and 7 d A transmission control means and 8 Information control means8a A ciphering system deciding means and 8b A cipher system transmitting means and 8c Key generation part8 d A control

means8e multimedia information transmitting meansand 8 f Execution information transmission system determination means9 A user information data base and 9a A contract information record9b user registration number9c A name and 9 d An address9e contract type9f multimedia information number9 g Multimedia execution control information9h multimedia information number9i multimedia execution control information10 multimedia-information database10a The name of a multimedia information record10b multimedia information numberand 10c multimedia informationand 10 d A real whereabouts type number and 10e Execution constraints10f multimedia information11 cipher-system databaseand 11a Cipher system record11b cipher system number and 11c The name of a cipher systemand 11 d Key generating means11e An encoding means and 11 f [A decoding means database and 13 / An encoding means database14 send dataand 14a / A cipher system number and 14b / Real whereabouts type database.] The multimedia information and 15 which were enciphered A decoding means and 11 g Usable area information and 12

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平10－177523

(43)公開日　平成10年(1998)６月30日

(51)Int.Cl.[6]		識別記号	FI		
Ｇ０６Ｆ	12/14	３２０	Ｇ０６Ｆ	12/14	３２０Ｂ
	12/00	５３７		12/00	５３７Ｈ
		５４７			５４７Ｄ
Ｇ０９Ｃ	1/00	６６０	Ｇ０９Ｃ	1/00	６６０Ｄ
Ｈ０４Ｌ	9/14		Ｈ０４Ｌ	9/00	６４１

審査請求　未請求　請求項の数10　ＯＬ　（全 18 頁）

(21)出願番号　特願平8－335594

(22)出願日　平成８年(1996)12月16日

(71)出願人　000006013
三菱電機株式会社
東京都千代田区丸の内二丁目２番３号

(72)発明者　藤井　誠司
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内

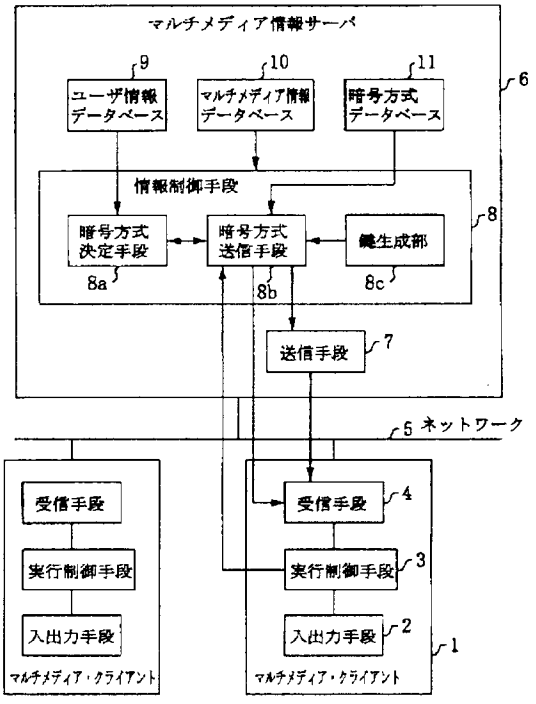
(74)代理人　弁理士　宮田　金雄　（外２名）

(54)【発明の名称】　マルチメディア情報システム

(57)【要約】

【課題】　マルチメディア情報への不正なアクセスを排除し、ユーザが契約条件に基づいてマルチメディア情報を実行することを保証する。

【解決手段】　マルチメディア情報サーバ６は、マルチメディア情報を暗号化する暗号化手段と暗号化マルチメディア情報を復号する復号手段とをユーザ情報データベース９に記憶されたユーザとの契約情報に基づいて決定する暗号方式決定手段８ａと、この暗号方式決定手段８ａにより決定された暗号化手段を用いて、マルチメディア情報データベース１０に記憶されたマルチメディア情報を暗号化し、この暗号化マルチメディア情報を送信する送信手段７とを備え、マルチメディア・クライアント１は、暗号方式決定手段８ａにより決定された復号手段を用いて、送信手段７により送信された暗号化マルチメディア情報を復号する受信手段４を備えた。



【特許請求の範囲】
【請求項１】　以下の要素を備えたマルチメディア情報システム。
（ａ）ユーザとの契約情報を記憶するユーザ情報記憶手段；
（ｂ）文字、図形、音声、静止画又は動画を含むマルチメディア情報を記憶するマルチメディア情報記憶手段；
（ｃ）以下の要素を備えたサーバ；
（ｃ１）上記マルチメディア情報を暗号化する暗号化手段と、この暗号化手段により暗号化されたマルチメディア情報を復号する復号手段とを、上記ユーザ情報記憶手段に記憶された上記契約情報に基づいて決定する暗号方式決定手段；
（ｃ２）この暗号方式決定手段により決定された暗号化手段を用いて、上記マルチメディア情報記憶手段に記憶されたマルチメディア情報を暗号化し、この暗号化したマルチメディア情報を送信する送信手段；
（ｄ）以下の要素を備え、上記サーバに上記マルチメディア情報の送信を要求するクライアント；
（ｄ１）上記暗号方式決定手段により決定された復号手段を用いて、上記送信手段により送信された暗号化マルチメディア情報を復号する受信手段。
【請求項２】　それぞれ異なる暗号化を行なう複数の暗号化手段とこの各暗号化手段により暗号化されたデータを復号する複数の復号手段とを記憶する暗号方式記憶手段を備え、
上記サーバは、上記暗号方式決定手段により決定された暗号化手段と復号手段とを上記暗号方式記憶手段より取り出し、この取り出した暗号化手段と復号手段とを送信する暗号方式送信手段を備え、
上記送信手段は、上記暗号方式送信手段により送信された暗号化手段を用いて暗号化し、
上記受信手段は、上記暗号方式送信手段により送信された復号手段を用いて復号することを特徴とする請求項１記載のマルチメディア情報システム。
【請求項３】　上記送信手段は、それぞれ異なる暗号化を行なう複数の暗号化手段を記憶する暗号方式記憶手段を備え、上記暗号方式決定手段により決定された暗号化手段を上記暗号方式記憶手段より取り出し、この取り出した暗号化手段を用いて暗号化し、
上記受信手段は、上記暗号方式記憶手段に記憶された暗号化手段により暗号化されたデータを復号する複数の復号手段を記憶する復号方式記憶手段を備え、上記暗号方式決定手段により決定された復号手段を上記復号方式記憶手段より取り出し、この取り出した復号手段を用いて復号することを特徴とする請求項１記載のマルチメディア情報システム。
【請求項４】　上記暗号化手段の使用可能な地域を示す地域情報を記憶する地域情報記憶手段を備え、
上記暗号方式決定手段は、上記ユーザ情報記憶手段に記憶された上記契約情報と上記地域情報記憶手段に記憶された上記地域情報とに基づいて、上記暗号化手段と上記復号手段とを決定することを特徴とする請求項１記載のマルチメディア情報システム。
【請求項５】　上記暗号方式決定手段は、新たに決定した暗号化手段と復号手段とを送信し、
上記送信手段は、
上記マルチメディア情報記憶手段に記憶されたマルチメディア情報を暗号化する暗号化手段を実行する複数の暗号化実行手段と、
上記暗号方式決定手段により送信された新たな暗号化手段を、実行中でない上記暗号化実行手段に実行させる暗号方式変更手段と、
上記暗号化実行手段により暗号化されたマルチメディア情報を送信する送信制御手段とを備え、
上記受信手段は、
上記送信制御手段により送信された暗号化マルチメディア情報を復号する復号手段を実行する複数の復号実行手段と、
上記暗号方式決定手段により送信された新たな復号手段を、実行中でない上記復号実行手段に実行させる復号方式変更手段とを備えたことを特徴とする請求項１記載のマルチメディア情報システム。
【請求項６】　上記送信制御手段は、上記暗号化実行手段により暗号化されたマルチメディア情報と暗号化するために使用した暗号化手段の種別とを格納した送信データを構築して送信し、
上記復号方式変更手段は、上記送信データを受信し、この受信したデータに格納された上記種別に基づいて上記マルチメディア情報を暗号化した暗号化手段を判別し、この暗号化手段に対応した復号手段を上記復号実行手段に実行させることを特徴とする請求項５記載のマルチメディア情報システム。
【請求項７】　以下の要素を備えたマルチメディア情報システム。
（ａ）ユーザとの契約情報を記憶するユーザ情報記憶手段；
（ｂ）文字、図形、音声、静止画又は動画を含むマルチメディア情報を記憶するマルチメディア情報記憶手段；
（ｃ）以下の要素を備えたサーバ；
（ｃ１）上記マルチメディア情報記憶手段に記憶されたマルチメディア情報を暗号化し、この暗号化したマルチメディア情報を送信する送信手段；
（ｃ２）上記マルチメディア情報の実行情報を受信し、この実行情報と上記ユーザ情報記憶手段に記憶された契約情報とを照合し、上記契約情報に基づいて上記マルチメディア情報を実行しているか否かを判別し、上記送信手段によるマルチメディア情報の送信を制御する制御手段；
（ｄ）以下の要素を備え、上記サーバに上記マルチメデ

ィア情報の送信を要求するクライアント；
（ｄ１）上記送信手段により送信された暗号化マルチメディア情報を復号する受信手段；
（ｄ２）この受信手段により復号されたマルチメディア情報を実行する実行手段；
（ｄ３）この実行手段の実行中の状態を示す実行情報を上記制御手段に送信する実行情報送信手段。
【請求項８】　上記サーバは、上記実行情報送信手段による上記実行情報の送信方式を上記ユーザ情報記憶手段に記憶された契約情報に基づいて決定する実行情報送信方式決定手段を備え、
上記実行情報送信手段は、上記実行情報送信方式決定手段により決定された送信方式により上記実行情報を送信することを特徴とする請求項７記載のマルチメディア情報システム。
【請求項９】　上記ユーザ情報記憶手段は、ユーザとの契約情報と、マルチメディア情報に対する実行制御情報とを記憶し、
上記制御手段は、上記受信した実行情報を上記ユーザ情報記憶手段に記憶された契約情報及び実行制御情報と照合し、上記契約情報及び上記実行制御情報に基づいて上記マルチメディア情報を実行しているか否かを判別し、上記マルチメディア情報の送信を制御することを特徴とする請求項７記載のマルチメディア情報システム。
【請求項１０】　上記マルチメディア情報記憶手段は、上記マルチメディア情報とこのマルチメディア情報の実行を制約する実行制約条件とを記憶し、
上記制御手段は、上記受信した実行情報を、上記ユーザ情報記憶手段に記憶された契約情報、及び、上記マルチメディア情報記憶手段に記憶された実行制約条件と照合し、上記契約情報及び上記実行制約条件に基づいて上記マルチメディア情報を実行しているか否かを判別し、上記マルチメディア情報の送信を制御することを特徴とする請求項７記載のマルチメディア情報システム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】この発明は、契約したユーザに文字、図形、音声、静止画又は動画からなるマルチメディア情報を暗号化して提供するマルチメディア情報システムに関するものである。
【０００２】
【従来の技術】図２０は、例えば特開平６－４４１２２号公報に示された従来のマルチメディア情報システムを示す概略構成図である。図において、５０は文字、図形、音声、静止画、動画などの各種メディアデータからなるマルチメディアファイルを暗号化して蓄積するマルチメディア情報蓄積部、５１はマルチメディア情報蓄積部５０に対するマルチメディアファイルの入出力を管理するマルチメディア情報管理部、５２はマルチメディアファイルの内容を表示する出力装置である。
【０００３】図２１はマルチメディア情報蓄積部５０に蓄積されるマルチメディアファイルの構成要素であるメディアデータの構成図である。図において、６０はメディアデータ、６０ａはユーザのセキュリティレベルに応じてアクセス可能なデータか否かを判別するための暗号化鍵情報、６０ｂはディスプレイ画面上での表示位置や表示する大きさを示す位置・大きさ情報、６０ｃはメディアデータのメディア種別を示すメディア種類情報、６０ｄは提示能力の異なるディスプレイ画面への対応のために入力時とは別のデータ形式のデータを付加した出力装置対応データである。このように、ユーザによるアクセスが可能か否かを判別するための暗号化鍵情報をメディアデータ毎に有しており、マルチメディアファイルを構成している一つ一つのメディアデータ単位でセキュリティレベルを変えることができる。
【０００４】次に動作について説明する。ユーザがマルチメディアファイルの出力をマルチメディア情報管理部５１に要求すると、マルチメディア情報管理部５１は、出力要求のあったマルチメディアファイルを構成しているメディアデータ６０をマルチメディア情報蓄積部５０から取り出す。次に、マルチメディア情報管理部５１は、ユーザのセキュリティレベルを解析し、各メディアデータ６０に含まれる暗号化鍵情報６０ａに基づき、そのユーザのセキュリティレベルでアクセス可能なメディアデータであるか否かを判別する。そして、ユーザがアクセス可能なメディアデータであると判別した時、このアクセス可能なメディアデータ６０のみを出力の対象とし、出力装置５２の提示能力に応じたデータ形式に変換して、出力装置５２へ出力する。
【０００５】
【発明が解決しようとする課題】従来のマルチメディア情報システムは、以上のように構成されており、暗号化したマルチメディア情報を蓄積し、ユーザへ送信している。そのため、長期間に渡って同じ暗号方式を使用することになり、契約しているユーザ以外の第三者によって通信データが盗聴され暗号方式を解読されるので、ユーザに送信しているマルチメディア情報へ第三者が不正にアクセスできるという問題点があった。
【０００６】また、ユーザのマルチメディア情報の実行に関する契約条件をマルチメディア情報を送信する前に確認するだけであり、マルチメディア情報の実行中は、ユーザが契約条件に基づいて正しく実行しているか否かがチエックできないため、マルチメディア情報を不正に実行できてしまうという問題点があった。
【０００７】また、日時、時間単位によるマルチメディア情報の実行、実行回数などの様々なユーザのマルチメディア情報の実行に関する契約条件に応じたマルチメディア情報の実行を制御することができないという問題点があった。
【０００８】この発明は、上記のような問題点を解消す

るためになされたものであり、第三者によるマルチメディア情報への不正なアクセスを排除し、ユーザが契約条件に基づいてマルチメディア情報を実行することを保証するマルチメディア情報システムを得ることを目的とする。

【０００９】

【課題を解決するための手段】請求項１記載のマルチメディア情報システムは、以下の要素を備えたものである。

（ａ）ユーザとの契約情報を記憶するユーザ情報記憶手段；

（ｂ）文字、図形、音声、静止画又は動画を含むマルチメディア情報を記憶するマルチメディア情報記憶手段；

（ｃ）以下の要素を備えたサーバ；

（ｃ１）上記マルチメディア情報を暗号化する暗号化手段と、この暗号化手段により暗号化されたマルチメディア情報を復号する復号手段とを、上記ユーザ情報記憶手段に記憶された上記契約情報に基づいて決定する暗号方式決定手段；

（ｃ２）この暗号方式決定手段により決定された暗号化手段を用いて、上記マルチメディア情報記憶手段に記憶されたマルチメディア情報を暗号化し、この暗号化したマルチメディア情報を送信する送信手段；

（ｄ）以下の要素を備え、上記サーバに上記マルチメディア情報の送信を要求するクライアント；

（ｄ１）上記暗号方式決定手段により決定された復号手段を用いて、上記送信手段により送信された暗号化マルチメディア情報を復号する受信手段。

【００１０】請求項２記載のマルチメディア情報システムは、それぞれ異なる暗号化を行なう複数の暗号化手段とこの各暗号化手段により暗号化されたデータを復号する複数の復号手段とを記憶する暗号方式記憶手段を備え、上記サーバは、上記暗号方式決定手段により決定された暗号化手段と復号手段とを上記暗号方式記憶手段より取り出し、この取り出した暗号化手段と復号手段とを送信する暗号方式送信手段を備え、上記送信手段は、上記暗号方式送信手段により送信された暗号化手段を用いて暗号化し、上記受信手段は、上記暗号方式送信手段により送信された復号手段を用いて復号するものである。

【００１１】請求項３記載のマルチメディア情報システムは、それぞれ異なる暗号化を行なう複数の暗号化手段を記憶する暗号方式記憶手段を有し、上記暗号方式決定手段により決定された暗号化手段を上記暗号方式記憶手段より取り出し、この取り出した暗号化手段を用いて暗号化する送信手段と、上記暗号方式記憶手段に記憶された暗号化手段により暗号化されたデータを復号する複数の復号手段を記憶する復号方式記憶手段を有し、上記暗号方式決定手段により決定された復号手段を上記復号方式記憶手段より取り出し、この取り出した復号手段を用いて復号する受信手段とを備えたものである。

【００１２】請求項４記載のマルチメディア情報システムは、上記暗号化手段の使用可能な地域を示す地域情報を記憶する地域情報記憶手段を備え、上記暗号方式決定手段は、上記ユーザ情報記憶手段に記憶された上記契約情報と上記地域情報記憶手段に記憶された上記地域情報とに基づいて、上記暗号化手段と上記復号手段とを決定するものである。

【００１３】請求項５記載のマルチメディア情報システムは、新たに決定した暗号化手段と復号手段とを送信する暗号方式決定手段を備え、上記送信手段は、上記マルチメディア情報記憶手段に記憶されたマルチメディア情報を暗号化する暗号化手段を実行する複数の暗号化実行手段と、上記暗号方式決定手段により送信された新たな暗号化手段を、実行中でない上記暗号化実行手段に実行させる暗号方式変更手段と、上記暗号化実行手段により暗号化されたマルチメディア情報を送信する送信制御手段とを備え、上記受信手段は、上記送信制御手段により送信された暗号化マルチメディア情報を復号する復号手段を実行する複数の復号実行手段と、上記暗号方式決定手段により送信された新たな復号手段を、実行中でない上記復号実行手段に実行させる復号方式変更手段とを備えたものである。

【００１４】請求項６記載のマルチメディア情報システムは、上記暗号化実行手段により暗号化されたマルチメディア情報と暗号化するために使用した暗号化手段の種別とを格納した送信データを構築して送信する送信制御手段と、上記送信データを受信し、この受信したデータに格納された上記種別に基づいて上記マルチメディア情報を暗号化した暗号化手段を判別し、この暗号化手段に対応した復号手段を上記復号実行手段に実行させる復号方式変更手段とを備えたものである。

【００１５】請求項７記載のマルチメディア情報システムは、以下の要素を備えたものである。

（ａ）ユーザとの契約情報を記憶するユーザ情報記憶手段；

（ｂ）文字、図形、音声、静止画又は動画を含むマルチメディア情報を記憶するマルチメディア情報記憶手段；

（ｃ）以下の要素を備えたサーバ；

（ｃ１）上記マルチメディア情報記憶手段に記憶されたマルチメディア情報を暗号化し、この暗号化したマルチメディア情報を送信する送信手段；

（ｃ２）上記マルチメディア情報の実行情報を受信し、この実行情報と上記ユーザ情報記憶手段に記憶された契約情報とを照合し、上記契約情報に基づいて上記マルチメディア情報を実行しているか否かを判別し、上記送信手段によるマルチメディア情報の送信を制御する制御手段；

（ｄ）以下の要素を備え、上記サーバに上記マルチメディア情報の送信を要求するクライアント；

（ｄ１）上記送信手段により送信された暗号化マルチメ

ディア情報を復号する受信手段；
（ｄ２）この受信手段により復号されたマルチメディア情報を実行する実行手段；
（ｄ３）この実行手段の実行中の状態を示す実行情報を上記制御手段に送信する実行情報送信手段。
【００１６】請求項８記載のマルチメディア情報システムは、上記実行情報送信手段による上記実行情報の送信方式を上記ユーザ情報記憶手段に記憶された契約情報に基づいて決定する実行情報送信方式決定手段を上記サーバに備え、上記実行情報送信手段は、上記実行情報送信方式決定手段により決定された送信方式により上記実行情報を送信するものである。
【００１７】請求項９記載のマルチメディア情報システムは、ユーザとの契約情報と、マルチメディア情報に対する実行制御情報とを記憶するユーザ情報記憶手段と、上記受信した実行情報を上記ユーザ情報記憶手段に記憶された契約情報及び実行制御情報と照合し、上記契約情報及び上記実行制御情報に基づいて上記マルチメディア情報を実行しているか否かを判別し、上記マルチメディア情報の送信を制御する制御手段とを備えたものである。
【００１８】請求項１０記載のマルチメディア情報システムは、上記マルチメディア情報とこのマルチメディア情報の実行を制約する実行制約条件とを記憶するマルチメディア情報記憶手段と、上記受信した実行情報を、上記ユーザ情報記憶手段に記憶された契約情報、及び、上記マルチメディア情報記憶手段に記憶された実行制約条件と照合し、上記契約情報及び上記実行制約条件に基づいて上記マルチメディア情報を実行しているか否かを判別し、上記マルチメディア情報の送信を制御する制御手段とを備えたものである。
【００１９】
【発明の実施の形態】
実施の形態１．以下、本発明を実施の形態に基づいて、図を参照しながら、説明する。図１は、実施の形態１のマルチメディア情報システムの構成図である。図において、１はマルチメディア情報の送信を要求するマルチメディア・クライアント、２はユーザからの要求を受け付けるとともに、マルチメディア情報の実行結果を出力する入出力手段、３はマルチメディア情報を実行し、実行結果を入出力手段２に送信する実行制御手段、４は暗号化されたマルチメディア情報を受信して復号し、実行制御手段３に送信する受信手段、５はネットワーク、６はマルチメディア情報サーバ、７はマルチメディア情報を暗号化し、マルチメディア・クライアント１へネットワーク５を経由して送信する送信手段、８は暗号方式を決定するとともに、マルチメディア情報の送信を制御する情報制御手段、９は契約しているすべてのユーザの契約情報を蓄積しているユーザ情報記憶手段としてのユーザ情報データベース、１０はマルチメディア情報サーバ６がサービスを提供するすべてのマルチメディア情報を蓄積しているマルチメディア情報記憶手段としてのマルチメディア情報データベース、１１はマルチメディア情報サーバ６で使用できるすべての暗号方式の鍵生成手段、暗号化手段及び復号手段を蓄積している暗号方式記憶手段としての暗号方式データベースである。
【００２０】情報制御手段８は、暗号方式決定手段８ａ、暗号方式送信手段８ｂ、鍵生成部８ｃから構成されている。暗号方式決定手段８ａは、ユーザ情報データベース９に蓄積されているユーザの契約情報に基づいてマルチメディア情報を送信する時に使用する暗号方式を決定する。暗号方式送信手段８ｂは、暗号方式決定手段８ａにより決定された暗号方式の鍵生成手段、暗号化手段及び復号手段を暗号方式データベース１１から取り出し、鍵生成手段は鍵生成部８ｃへ、暗号化手段は送信手段７へ、復号手段は受信手段４へ送信する。鍵生成部８ｃは、暗号方式送信手段８ｂにより送信された鍵生成手段を用いて、暗号化鍵と復号鍵を生成する。
【００２１】本システムは、図示したように、マルチメディア情報サーバ６と、複数のマルチメディア・クライアント１とが、ネットワーク５に接続されており、マルチメディア情報サーバ６は、マルチメディア・クライアント１から要求されたマルチメディア情報をマルチメディア情報データベース１０より取り出して暗号化し、マルチメディア・クライアント１に送信するものである。
【００２２】図２は、ユーザ情報データベース９に蓄積されている契約情報の構成を示す構成図である。図において、９ａはユーザとの契約情報レコード、９ｂはユーザ登録番号、９ｃはユーザの氏名、９ｄはユーザの住所、９ｅはユーザとの契約タイプである。契約タイプ９ｅは暗号方式を決定するための情報である。
【００２３】図３は、マルチメディア情報データベース１０に蓄積されているマルチメディア情報の構成を示す構成図である。図において、１０ａはマルチメディア情報レコード、１０ｂはマルチメディア情報を一意に識別するためのマルチメディア情報番号、１０ｃはマルチメディア情報の名称、１０ｄはマルチメディア情報の実行手段を示す実行方式番号、１０ｆはマルチメディア情報である。
【００２４】図４は、暗号方式データベース１１に蓄積されている暗号方式の構成を示す構成図である。図において、１１ａは暗号方式レコード、１１ｂは暗号方式を一意に識別するための暗号方式番号、１１ｃは暗号方式の名称、１１ｄは暗号化鍵と復号鍵を生成する鍵生成手段、１１ｅはマルチメディア情報を暗号化する暗号化手段、１１ｆは暗号化されたマルチメディア情報を復号する復号手段である。
【００２５】次に動作ついて、図５のフローチャートに基づいて説明する。入出力手段２に表示されているマルチメディア情報番号１０ａとマルチメディア情報名称１

０ｃの中から、ユーザが一つのマルチメディア情報番号１０ａを選択すると（ステップＳ１）、実行制御手段３は、ユーザにより入力されたユーザ登録番号９ｂと、選択されたマルチメディア情報番号１０ａとを、マルチメディア情報サーバ６の暗号方式送信手段８ｂへ送信する（ステップＳ２）。暗号方式送信手段８ｂは、ユーザ登録番号９ｂを暗号方式決定手段８ａへ出力する（ステップＳ３）。

【００２６】暗号方式決定手段８ａは、ユーザ登録番号９ｂを検索条件としてユーザ情報データベース９からユーザの契約情報レコード９ａを取得し（ステップＳ４）、取得した契約情報レコード９ａ中の契約タイプ９ｅに基づいて暗号方式を決定し、決定した暗号方式の暗号方式番号１１ｂを暗号方式送信手段８ｂへ出力する（ステップＳ５）。

【００２７】暗号方式送信手段８ｂは、暗号方式番号１１ｂを検索条件として、暗号方式データベース１１から鍵生成手段１１ｄ、暗号化手段１１ｅ及び復号手段１１ｆを取得する（ステップＳ６）。暗号方式送信手段８ｂは、鍵生成手段１１ｄを鍵生成部８ｃへ出力し（ステップＳ７）、鍵生成部８ｃは、この出力された鍵生成手段１１ｄを使用して、暗号化鍵と復号鍵を生成し、暗号方式送信手段８ｂへ出力する（ステップＳ８）。暗号方式送信手段８ｂは、鍵生成部８ｃにより生成された暗号化鍵と、暗号方式データベース１１から取得した暗号化手段１１ｅとを送信手段７へ出力し（ステップＳ９）、鍵生成部８ｃにより生成された復号鍵と、暗号方式データベース１１から取得した復号手段１１ｆを受信手段４へ送信する（ステップＳ１０）。

【００２８】そして次に、暗号方式送信手段８ｂは、ステップＳ２で送信されたマルチメディア情報番号１０ａを検索条件として、ユーザが選択したマルチメディア情報１０ｆをマルチメディア情報データベース１０から取り出し、ブロックに分割して送信手段７へ出力する（ステップＳ１１）。送信手段７は、ステップＳ９で出力された暗号化鍵と暗号化手段１１ｅとを用いて、マルチメディア情報１０ｆの各ブロックを暗号化し、受信手段４へ送信する（ステップＳ１２）。

【００２９】受信手段４は、受信した暗号化マルチメディア情報１０ｆの各ブロックを、ステップＳ１０で送信された復号鍵と復号手段１１ｆとを用いて復号し、実行制御手段３へ送信する（ステップＳ１３）。実行制御手段３は、復号されたマルチメディア情報１０ｆを実行し、実行結果を入出力手段２へ出力する（ステップＳ１４）。

【００３０】以上のように、この実施の形態によれば、暗号方式データベース１１に蓄積されている多数の暗号方式の中から、ユーザの契約タイプに基づいて暗号方式を選択し、ユーザ毎に暗号方式を変更しているので、第三者は暗号方式の推測が困難であるため、不正なアクセスが排除できるという効果がある。

【００３１】なお、この実施の形態では、暗号方式決定手段８ａが暗号方式を決定し、暗号方式送信手段８ｂが鍵生成手段、暗号化手段及び復号手段を送信する形態を示したが、暗号方式決定手段８ａが暗号方式送信手段８ｂの機能を有し、決定した暗号方式に対応する各手段を送信するように構成することも出来る。

【００３２】実施の形態２．送信手段７で実行する暗号化手段や、受信手段４で実行する復号手段が変更できない場合には、図６に示すように、複数の異なる暗号方式の送信手段７と受信手段４とを用いて、情報制御手段８が送信手段７を切り替え、実行制御手段３へ同じ暗号方式の受信手段４を使用するように命令して切り替えることより、マルチメディア情報システムを実現することもできる。

【００３３】実施の形態３．また、ネットワークを経由して復号手段１１ｆを送信する場合、第三者に復号手段１１ｆを盗まれる可能性があることや、復号手段１１ｆを受信手段４へ送信する時間を短縮するため、図７に示すように、マルチメディア・クライアント側に復号手段だけを蓄積した復号手段データベース１２を分散して配置することもできる。

【００３４】実施の形態４．さらに、図８に示すように、マルチメディア情報サーバ側の送信手段７が暗号化手段データベース１３を持ち、マルチメディア・クライアント側の受信手段４が復号手段データベース１２を内部に持つように構成することもできる。

【００３５】実施の形態５．実施の形態１では、ユーザとの契約情報中の契約タイプに基づいて暗号方式を決定したが、契約タイプに合致する暗号方式の候補が複数残った場合に暗号方式を１つに決定するためには、契約タイプ以外の情報が必要になる。

【００３６】ユーザとマルチメディア情報サーバとの間で暗号化したデータを送受信するとき、使用可能な暗号方式が居住地域の法律によって制限されることがある。マルチメディア・クライアントが存在する地域で使用可能な暗号方式と、マルチメディア情報サーバが存在する地域で使用可能な暗号方式とで、まったく同じ暗号方式が使用できるとは限らないので、両方の場所で使用できる暗号方式を決定する必要があるが、これはユーザ個人との契約条件だけでは判断できない。そこで、この実施の形態では、暗号方式データベースを図９に示す構造にする。図９に示した暗号方式データベースは、図４に示した暗号方式データベースに対して、各暗号方式の使用可能地域を示す使用可能地域情報１１ｇを追加したものである。

【００３７】この実施の形態のマルチメディア情報システムの構成は、実施の形態１で説明した図１の構成と同様であるが、暗号方式決定手段８ａにおける暗号方式決定の動作が実施の形態１のものと異なる。異なる動作

は、実施の形態１で説明したステップＳ４、Ｓ５である。異なる動作を次に説明する。この実施の形態では、暗号方式決定手段８ａは、ユーザ登録番号９ｂを検索条件としてユーザ情報データベース９からユーザの契約情報レコード９ａを取得する。次に、図８に示した暗号方式データベース１１から暗号方式レコード１１ａを取り出す。そして、取得した契約情報レコード９ａ中の住所９ｄが、暗号方式レコード１１ａ中の使用可能地域情報１１ｇに合致するか否かを調べる。合致する暗号方式が複数である場合は、その中からユーザの契約情報レコード９ａ中の契約タイプ９ｅに合致する暗号方式を決定し、決定した暗号方式の暗号方式番号１１ｂを暗号方式送信手段８ｂへ出力する。

【００３８】以上のように、この実施の形態によれば、ユーザの契約タイプと、暗号方式の使用可能地域情報とに基づいて暗号方式を決定するので、使用できる暗号方式が地域によって異なる場合にも、暗号方式を選択することができる。

【００３９】実施の形態６．図１０は、実施の形態６のマルチメディア情報システムの構成図である。図において、実行制御手段３と受信手段４は、図１に示したものと同様にマルチメディア・クライアントを構成し、送信手段７と情報制御手段８は、図１に示したものと同様にマルチメディア情報サーバを構成する。

【００４０】情報制御手段８において、暗号方式決定手段８ａは、暗号方式が変更になったときは、新たに暗号方式を決定し、暗号方式送信手段８ｂは、新たな暗号方式に基づいて、鍵生成手段、暗号化手段及び復号手段を図１に示した暗号方式データベース１１から取り出し、鍵生成手段は鍵生成部８ｃへ、暗号化手段は送信手段７へ、復号手段は受信手段４へ送信する。送信手段７は、暗号方式変更手段７ａ、暗号化実行手段７ｂ、７ｃ及び送信制御手段７ｄから構成されている。暗号方式変更手段７ａは、暗号方式送信手段８ｂにより送信された新たな暗号化手段に基づいて、送信手段７で使用する暗号化実行手段７ｂ、７ｃを切り替える。暗号化実行手段７ｂ、７ｃは、暗号方式送信手段８ｂから送信された暗号化手段を実行するものであり、送信制御手段７ｄから出力されるデータを暗号化し、その結果を送信制御手段７ｄへ出力する。送信制御手段７ｄは、情報制御手段８より出力されたマルチメディア情報のブロックを暗号化実行手段７ｂ又は７ｃに出力し、暗号化実行手段７ｂ、７ｃにより暗号化されたマルチメディア情報を受信手段４へ送信する。

【００４１】受信手段４は、復号方式変更手段４ａ、復号実行手段４ｂ、４ｃ及び受信制御手段４ｄから構成されている。復号方式変更手段４ａは、暗号方式送信手段８ｂにより送信された新たな復号手段に基づいて、受信手段４で使用する復号実行手段４ｂ、４ｃを切り替える。復号実行手段４ｂ、４ｃは、暗号方式送信手段８ｂから送信された復号手段を実行するものであり、受信制御手段４ｄから出力されるデータを復号して、その結果を受信制御手段４ｄへ出力する。受信制御手段４ｄは、送信制御手段７ｄより出力された暗号化マルチメディア情報を復号実行手段４ｂ又は４ｃに出力し、復号実行手段４ｂ、４ｃにより復号されたマルチメディア情報を実行制御手段３へ送信する。

【００４２】次に、動作について、図１１のフローチャートに基づいて説明する。暗号方式送信手段８ｂは、暗号方式決定手段８ａにより決定された暗号化鍵と暗号化手段を暗号方式変更手段７ａへ送信する（ステップＳ２０）。暗号方式変更手段７ａは、受信した暗号化鍵と暗号化手段を暗号化実行手段７ｂへ出力し、暗号化実行手段７ｂを使用して暗号化するように設定する（ステップＳ２１）。暗号方式送信手段８ｂは、復号鍵と復号手段受信手段４の復号方式変更手段４ａへ送信する（ステップＳ２２）。復号方式変更手段４ａは、受信した復号鍵と復号手段を復号実行手段４ｂへ出力し、復号実行手段４ｂを使用して復号するように設定する（ステップＳ２３）。

【００４３】情報制御手段８は、マルチメディア情報をブロックに分割し、送信制御手段７ｄへブロックを送信する（ステップＳ２４）。送信制御手段７ｄは、受信したブロックを、暗号化実行手段７ｂへ出力する（ステップＳ２５）。暗号化実行手段７ｂは、ステップＳ２１で出力された暗号化鍵と暗号化手段を使用してブロックを暗号化し、送信制御手段７ｄへ出力する（ステップＳ２６）。送信制御手段７ｄは、暗号化されたブロックをネットワーク５を経由して受信制御手段４ｄへ送信する（ステップＳ２７）。

【００４４】受信制御手段４ｄは、ネットワーク５から暗号化されたマルチメディア情報のブロックを受信すると、復号実行手段４ｂへ出力する（ステップＳ２８）。復号実行手段４ｂは、ステップＳ２３で出力された復号鍵と復号手段を使用して暗号化ブロックを復号し、受信制御手段４ｄへ出力する（ステップＳ２９）。受信制御手段４ｄは、復号したブロックを実行制御手段３へ送信する（ステップＳ３０）。

【００４５】次に、マルチメディア情報の実行中に暗号方式を変更する場合の動作を、図１２のフローチャートに基づいて説明する。情報制御手段８は、現在使用している暗号方式が変更になると、マルチメディア情報のブロックの送信制御手段７ｄへの送信を停止する（ステップＳ４０）。暗号方式送信手段８ｂは、暗号方式決定手段８ａにより決定された変更後の暗号化鍵と暗号化手段を暗号方式変更手段７ａへ送信する（ステップＳ４１）。暗号方式変更手段７ａは、受信した暗号化鍵と暗号化手段を暗号化実行手段７ｃへ出力し、次に受信するブロックは暗号化実行手段７ｃを使用して暗号化するように設定する（ステップＳ４２）。暗号方式送信手段８

ｂは、暗号方式決定手段８ａにより決定された変更後の復号鍵と復号手段を復号方式変更手段４ａへ送信する（ステップＳ４３）。復号方式変更手段４ａは、受信した復号鍵と復号手段を復号実行手段４ｃへ出力し、次に受信する暗号化ブロックは復号実行手段４ｃを使用して復号するように設定する（ステップＳ４４）。

【００４６】情報制御手段８は、送信の停止を解除し、マルチメディア情報をブロックに分割し、送信制御手段７ｄへブロックの送信を再開する（ステップＳ４５）。送信制御手段７ｄは、受信したブロックを暗号化実行手段７ｃへ出力する（ステップＳ４６）。暗号化実行手段７ｃは、ステップＳ４２で出力された変更後の暗号化鍵と暗号化手段を使用て、ブロックを暗号化し、送信制御手段７ｄへ出力する（ステップＳ４７）。送信制御手段７ｄは、暗号化されたブロックをネットワーク５を経由して受信制御手段４ｄへ送信する（ステップＳ４８）。

【００４７】受信制御手段４ｄは、ネットワーク５から暗号化されたマルチメディア情報のブロックを受信すると、復号実行手段４ｃへ出力する（ステップＳ４９）。復号実行手段４ｃは、ステップＳ４２で出力された復号鍵と復号手段を使用して、ブロックを復号し、受信制御手段４ｄへ出力する（ステップＳ５０）。受信制御手段４ｄは、復号したブロックを実行制御手段３へ送信する（ステップＳ５１）。

【００４８】以上のように、この実施の形態によれば、使用する暗号方式を動的に変更することができるので、マルチメディア情報サーバに暗号方式を追加する場合に、システムを構成するハードウェアを変更する必要が無いという効果がある。

【００４９】なお、この実施の形態では、暗号方式決定手段８ａが新たな暗号方式を決定し、暗号方式送信手段８ｂは、新たな暗号方式に基づいて、鍵生成手段、暗号化手段及び復号手段を送信する形態を示したが、暗号方式決定手段８ａが暗号方式送信手段８ｂの機能を有し、新たな暗号方式に対応する各手段を送信するように構成することも出来る。

【００５０】この実施の形態では、図１０に示したように、送信手段７内の暗号化実行手段７ｂ、７ｃ、及び、受信手段４内の復号実行手段４ｂ、４ｃは、２つに限らず、２つ以上であっても良い。一度使用した暗号化方式は、暗号化実行手段７ｂ、７ｃ及び復号実行手段４ｂ、４ｃに保存されていて、再度同じ暗号方式が使用されるときに、新しい暗号化鍵を暗号化実行手段７ｂ、７ｃへ出力し、新しい復号鍵を復号実行手段４ｂ、４ｃへ出力して、暗号化実行手段７ｂ、７ｃ内にある暗号化手段と、復号実行手段４ｂ、４ｃ内にある復号手段を再使用する。

【００５１】また、暗号化実行手段７ｂ、７ｃ、又は、復号実行手段４ｂ、４ｃが既に使用中で、未使用のものがないときは、使用頻度の低い暗号化実行手段７ｂ、７ｃ、又は、復号実行手段４ｂ、４ｃを使用するように制御する。

【００５２】実施の形態７．実施の形態７は、図１３に示すように、暗号化されたマルチメディア情報１４ｂのブロックと、その暗号化に使用した暗号方式の暗号方式番号１４ａとによって構成される送信データ１４を作成するものである。システムの構成は、実施の形態６で説明した図１０のものと同様であるが、送信制御手段７ｄと受信制御手段４ｄの処理が異なる。送信制御手段７ｄは、図１３に示した送信データを作成し、ネットワーク５を介して受信制御手段４ｄへ送信し、これを受信した受信制御手段４ｄは、暗号化されたマルチメディア情報１４ｂを復号する復号手段を、暗号方式番号１４ａにより決定し、復号実行手段４ｂ又は復号実行手段４ｃのいずれかに復号を実行させる。

【００５３】実施の形態８．図１４は、実施の形態８のマルチメディア情報システムの構成図である。図において、１５はマルチメディア情報を実行するための複数の手段を実行方式番号とともに蓄積している実行方式データベースである。ユーザ情報データベース９は図２に示すものであり、マルチメディア情報データベース１０は図３に示すものである。実行制御手段３は、実行情報制御手段３ａと実行手段３ｂとから構成されている。実行手段３ｂは、受信手段４により復号されたマルチメディア情報を実行し、実行結果を入出力手段２に送信する。実行情報制御手段３ａは、一定時間間隔で、マルチメディア情報を実行している時の実行情報と、入出力手段２により出力されたユーザの要求とをマルチメディア情報サーバ６に送信する。実行情報には、ユーザ登録番号９ｂ、実行中のマルチメディア情報番号１０ｂ、現在までのマルチメディア情報の実行の累積時間が含まれている。情報制御手段８は、制御手段８ｄとマルチメディア情報送信手段８ｅとから構成されている。制御手段８ｄは、実行情報制御手段３ａにより送信されたマルチメディア情報の実行情報を受信してその情報を解析し、マルチメディア情報送信手段８ｅを制御する。マルチメディア情報送信手段８ｅは、マルチメディア情報データベース１０からマルチメディア情報を取得し、送信手段７へ送信する。送信手段７は、マルチメディア情報を暗号化して受信手段４へ送信する。

【００５４】次に、マルチメディア情報の実行を開始するまでの動作を図１５のフローチャートに基づいて説明する。ユーザが一つのマルチメディア情報を選択すると、実行情報制御手段３ａがユーザ登録番号９ｂとマルチメディア情報番号１０ｂとを制御手段８ｄへ送信する（ステップＳ６０）。制御手段８ｄは、ユーザ登録番号９ｂを検索条件としてユーザ情報データベース９からユーザの契約情報レコード９ａを取り出し、契約タイプ９ｅから、要求のあったマルチメディア情報を実行可能であるか、また、要求の合った日時で実行が開始できるか

判定する（ステップＳ６１）。制御手段８ｄは、マルチメディア情報の実行開始が可能であると判定すると、マルチメディア情報番号１０ｂを検索条件としてマルチメディア情報データベース１０からマルチメディア情報レコード１０ａを取り出し、実行方式番号１０ｄを取得する（ステップＳ６２）。次に、制御手段８ｄは、実行方式番号１０ｄを検索条件として、実行方式データベース１５から実行手段を取り出し、実行情報制御手段３ａへ送信する（ステップＳ６３）。実行情報制御手段３ａは、受信した実行手段を実行手段３ｂへ出力する（ステップＳ６４）。制御手段８ｄは、マルチメディア情報送信手段８ｅへマルチメディア情報番号１０ｂを出力する（ステップＳ６５）。マルチメディア情報送信手段８ｅは、マルチメディア情報番号１０ｂを検索条件としてマルチメディア情報データベース１０からマルチメディア情報レコード１０ａを取り出し、ブロックに分割して送信手段７へ送信する（ステップＳ６６）。

【００５５】送信手段７は受信したブロックを暗号化し、ネットワーク５を経由して、受信手段４へ送信する（ステップＳ６７）。受信手段４は受信したブロックを復号して、実行手段３ｂへ送信する（ステップＳ６８）。実行手段３ｂは、実行準備が終了したメッセージを入出力手段２へ出力する（ステップＳ６９）。ユーザは入力手段２から、マルチメディア情報の実行開始を入力する（ステップＳ７０）。実行情報制御手段３ａは、実行開始の指示を受け取ると、マルチメディア情報の実行の開始のメッセージを制御手段８ｄへ送信し、実行の累積時間の計数を開始する（ステップＳ７１）。制御手段８ｄは、マルチメディア情報の実行の開始のメッセージを受信すると、マルチメディア情報送信手段８ｅへ送信開始メッセージを出力する（ステップＳ７２）。

【００５６】次に、マルチメディア情報の実行中の動作を図１６のフローチャートに基づいて説明する。マルチメディア情報送信手段８ｅは、マルチメディア情報番号１０ｂを検索条件としてマルチメディア情報データベース１０からマルチメディア情報を取り出してブロックに分割し、送信手段７へ送信する（ステップＳ８０）。制御手段８ｄは、マルチメディア情報の実行の累積時間の計数を開始し、実行情報の受信を待つ（ステップＳ８１）。送信手段７は、マルチメディア情報のブロックを暗号化し、ネットワーク５を経由して、受信手段４へ送信する（ステップＳ８２）。受信手段４は、受信したブロックを復号し、実行手段３ｂへ送信する（ステップＳ８３）。実行手段３ｂは、受信手段４からマルチメディア情報を受信すると、マルチメディア情報を実行し、実行結果を入出力手段２へ出力する（ステップＳ８４）。

【００５７】ステップＳ８０～Ｓ８４の動作を繰り返しているときに一定時間が経過すると（ステップＳ８５）、実行情報制御手段３ａは、現在までのマルチメディア情報の実行の累積時間をセットした実行情報を制御手段８ｄに送信する（ステップＳ８６）。制御手段８ｄは、制御手段８ｄが計数した実行の累積時間と実行情報にセットされている累積時間との差の絶対値を計算し、その差の絶対値が制御手段８ｄが保有している誤差の範囲を超えているか否かをチエックし（ステップＳ８７）、超えている場合は（ステップＳ８８）、契約タイプ９ｅに一致しない不正な実行が検出されたと判断し、送信の停止を示すメッセージをマルチメディア情報送信手段８ｅへ出力する（ステップＳ８８）。マルチメディア情報送信手段８ｅはマルチメディア情報の送信を中止する（ステップＳ８９）。

【００５８】以上のように、この実施の形態によれば、マルチメディア情報の実行累積時間を契約タイプに基づいてチエックし、所定の時間を超えているときには送信を停止するので、マルチメディア情報の実行中に、契約条件に違反する不正なマルチメディア情報の実行を防止する効果がある。

【００５９】実施の形態９．図１７は、実施の形態９のマルチメディア情報システムの構成図である。図において、８ｆは実行情報を実行情報制御手段３ａから送信するタイミングを制御手段８ｄからの要求で決定する実行情報送信方式決定手段である。

【００６０】次に、動作について説明する。ユーザが一つのマルチメディア情報を選択すると、実行情報制御手段３ａがユーザ登録番号９ｂとマルチメディア情報番号１０ｂを制御手段８ｄへ送信する。制御手段８ｄは、ユーザ情報データベース９からユーザ登録番号９ｂを検索条件として、ユーザの契約情報レコード９ａを取り出し、契約タイプ９ｅを実行情報送信方式決定手段８ｆへ出力する。実行情報送信方式決定手段８ｆは、実行情報制御手段３ａで使用できる実行情報送信方式の番号リストを内部に持っており、契約タイプ９ｅからリストの中の一つを選択し、選択した方式の方式番号を制御手段８ｄへ出力する。制御手段８ｄは、方式番号を実行情報制御手段３ａへ送信する。実行情報制御手段３ａは、方式番号を受信すると、実行情報を方式番号の実行情報送信方式に基づいて、制御手段８ｄへ送信する。

【００６１】なお、実行情報の送信方式は、情報実行中にユーザの要求があった時のみ実行情報を送信する方式方式、ある一定の時間間隔で実行情報を送信する方式、あるいは、不規則な時間間隔で実行情報を送信する方式などがある。

【００６２】以上のように、この実施の形態によれば、マルチメディア情報サーバへ実行情報を送信する方式を変更することにより、実行情報を送る時間にユーザおよび第三者が盗聴し虚の実行情報を送信することができなくなるので、不正なマルチメディア情報の実行を防止する効果がある。

【００６３】実施の形態１０．図１８は、実施の形態１０におけるユーザ情報データベースの構成図であり、図

２に示したユーザ情報データベースに対して、マルチメディア情報番号９ｆ、９ｈとマルチメディア実行制御情報９ｇ、９ｉとを追加し、ユーザがサービスを契約しているマルチメディア情報の番号と実行制御情報とを保持している。この実施の形態のシステム構成は、図１４に示したものと同様である。

【００６４】次に、動作について説明する。ユーザが一つのマルチメディア情報を選択すると、実行情報制御手段３ａがユーザ登録番号９ｂとマルチメディア情報番号１０ｂを制御手段８ｄへ送信する。制御手段８ｄは、ユーザ情報データベース９からユーザ登録番号９ｂを検索条件として、ユーザの契約情報レコード９ａを取り出し、その中のマルチメディア情報番号９ｆ、９ｈに、ユーザが要求しているマルチメディア情報番号１０ｂが含まれているか否かを確認する。制御手段８ｄは、ユーザが要求している番号を見つけると、マルチメディア情報番号９ｆ、９ｈに対応するマルチメディア実行制御情報９ｇ、９ｉに基づいて、マルチメディア情報の実行の開始が可能であるか否かを判定する。ユーザが要求している番号がない場合は、契約タイプ９ｅに基づいて、要求のあったマルチメディア情報を実行可能であるか否か、また、要求のあった日時で実行の開始が可能であるか否かを判定する。

【００６５】マルチメディア情報の実行中にユーザの制御要求が発生すると、実行情報制御手段３ａはその要求を実行情報として、制御手段８ｄへ送信する。制御手段８ｄは、マルチメディア実行制御情報９ｇ、９ｉに基づいて、この要求が実行可能であるか否かを判定する。可能であると判定されれば、実行情報制御手段３ａへ実行可能であるメッセージを送信する。実行情報制御手段３ａは、実行手段３ｂをユーザの要求に基づいて制御する。不可能であると判定されれば、実行情報制御手段３ａへ実行不可であるメッセージを送信する。実行情報制御手段３ａは、入出力装置１へユーザの要求は破棄されたこと示すメッセージを出力する。

【００６６】以上のように、この実施の形態によれば、ユーザ情報データベース中にユーザが契約しているマルチメディア情報の実行制御情報を格納し、この実行制御情報に基づいてマルチメディア情報を実行しているか否かを判別し、マルチメディア情報の送信を制御するので、契約条件に違反する不正なマルチメディア情報の実行を防止する効果がある。

【００６７】実施の形態１１．図１９は、実施の形態１１におけるマルチメディア情報データベースの構成図であり、図３に示したマルチメディア情報データベースに対して、マルチメディア情報の実行を制約する実行制約条件１０ｅを追加している。この実施の形態のシステム構成は、図１４に示したものと同様である。

【００６８】次に、動作について説明する。ユーザが一つのマルチメディア情報を選択すると、実行情報制御手段３ａがユーザ登録番号９ｂとマルチメディア情報番号１０ｂを制御手段８ｄへ送信する。制御手段８ｄは、ユーザ登録番号９ｂを検索条件として、ユーザ情報データベース９からユーザの契約情報レコード９ａ中のユーザの契約タイプ９ｅを取り出す。また、制御手段８ｄは、マルチメディア情報番号１０ｂを検索条件として、マルチメディア情報データベース１０からマルチメディア情報レコード１０ａ中の実行制約条件１０ｅを取り出し、ユーザの契約タイプ９ｅが実行制約条件１０ｅに含まれているか否かを確認する。含まれている場合は、契約タイプ９ｅから、要求のあったマルチメディア情報を実行可能であるか否か、また、要求の合った日時で実行の開始が可能であるか否かを判定する。含まれていない場合は、ユーザからの要求を破棄し、ユーザからの要求が破棄されたことを示すメッセージを実行情報制御手段３ａへ送信する。実行情報制御手段３ａは、入出力装置１へユーザの要求が破棄されたこと示すメッセージを出力する。

【００６９】以上のように、この実施の形態によれば、マルチメディア情報データベース中にマルチメディア情報を実行するための実行制約条件を格納し、この実行制約条件に基づいてマルチメディア情報を実行しているか否かを判別し、マルチメディア情報の送信を制御するので、契約条件に違反する不正なマルチメディア情報の実行を防止する効果がある。

【００７０】

【発明の効果】以上のように、請求項１記載の発明よれば、マルチメディア情報を暗号化する暗号化手段と、この暗号化手段により暗号化されたマルチメディア情報を復号する復号手段とを、ユーザとの契約情報に基づいて決定することにより、ユーザ毎に暗号方式を変更しているので、第三者は暗号方式の推測が困難であるため、マルチメディア情報への不正なアクセスが排除できるという効果がある。

【００７１】請求項２記載の発明によれば、複数の暗号化手段と複数の復号手段とを記憶する暗号方式記憶手段を備え、暗号化手段と復号手段とをユーザとの契約情報に基づいて決定することにより、ユーザ毎に暗号方式を変更しているので、第三者は暗号方式の推測が困難であるため、マルチメディア情報への不正なアクセスが排除できるという効果がある。

【００７２】請求項３記載の発明によれば、暗号化マルチメディア情報を送信する送信手段は、複数の暗号化手段を記憶する暗号方式記憶手段を備え、暗号化マルチメディア情報を復号する受信手段は、複数の復号手段を記憶する復号方式記憶手段を備えたので、復号手段をサーバからクライアントに送信する必要が無いため、復号手段の送信時間分を短縮できるという効果がある。

【００７３】請求項４記載の発明によれば、暗号化手段の使用可能な地域を示す地域情報を記憶する地域情報記

憶手段を備え、ユーザとの契約情報と地域情報とに基づいて暗号化手段と復号手段とを決定するので、使用できる暗号方式が地域によって異なる場合にも、暗号方式を選択できるという効果がある。

【００７４】請求項５記載の発明によれば、サーバの送信手段は、実行中でない暗号化実行手段に暗号化を実行させる暗号方式変更手段を備え、クライアントの受信手段は、実行中でない復号実行手段に復号を実行させる復号方式変更手段を備えたことにより、使用する暗号方式を動的に変更することができるので、暗号方式を追加する場合に、システムを構成するハードウェアを変更する必要が無いという効果がある。

【００７５】請求項６記載の発明によれば、暗号化マルチメディア情報の送信データ中に使用した暗号化手段の種別を格納することにより、送信データから暗号方式を知ることができるので、暗号方式をクライアントへ通知する必要が無く、時間が短縮できるという効果がある。

【００７６】請求項７記載の発明によれば、クライアント側でのマルチメディア情報の実行状態を示す実行情報をユーザとの契約情報と照合し、契約に基づいてマルチメディア情報を実行しているか否かを判別するので、契約条件に違反する不正なマルチメディア情報の実行を防止する効果がある。

【００７７】請求項８記載の発明によれば、クライアントからサーバへの実行情報送信方式をユーザとの契約情報に基づいて決定することにより、実行情報を送る時間に盗聴し虚の実行情報を送信することができなくなるので、契約条件に違反する不正なマルチメディア情報の実行を防止する効果がある。

【００７８】請求項９記載の発明によれば、ユーザ情報記憶手段中にユーザが契約しているマルチメディア情報の実行制御情報を格納し、この実行制御情報に基づいてマルチメディア情報を実行しているか否かを判別し、マルチメディア情報の送信を制御するので、契約条件に違反する不正なマルチメディア情報の実行を防止する効果がある。

【００７９】請求項１０記載の発明によれば、マルチメディア情報記憶手段中にマルチメディア情報の実行を制約する実行制約条件を格納し、この実行制約条件に基づいてマルチメディア情報を実行しているか否かを判別し、マルチメディア情報の送信を制御するので、契約条件に違反する不正なマルチメディア情報の実行を防止する効果がある。

【図面の簡単な説明】

【図１】　実施の形態１のマルチメディア情報システムの構成図である。

【図２】　ユーザ情報データベースの構成図である。

【図３】　マルチメディア情報データベースの構成図である。

【図４】　暗号方式データベースの構成図である。

【図５】　実施の形態１のマルチメディア情報システムの動作を示すフローチャートである。

【図６】　実施の形態２のマルチメディア情報システムの構成図である。

【図７】　実施の形態３のマルチメディア情報システムの構成図である。

【図８】　実施の形態４のマルチメディア情報システムの構成図である。

【図９】　実施の形態５の暗号方式データベースの構成図である。

【図１０】　実施の形態６のマルチメディア情報システムの構成図である。

【図１１】　実施の形態６のマルチメディア情報システムの動作を示すフローチャートである。

【図１２】　実施の形態６のマルチメディア情報システムにおける暗号方式を変更する場合の動作を示すフローチャートである。

【図１３】　実施の形態７におけるマルチメディア情報サーバの送信データの構成図である。

【図１４】　実施の形態８のマルチメディア情報システムの構成図である。

【図１５】　実施の形態８のマルチメディア情報システムの動作を示すフローチャートである。

【図１６】　実施の形態８のマルチメディア情報システムにおけるマルチメディア情報実行中の動作を示すフローチャートである。

【図１７】　実施の形態９のマルチメディア情報システムの構成図である。

【図１８】　実施の形態１０におけるユーザ情報データベースの構成図である。

【図１９】　実施の形態１１におけるマルチメディア情報データベースの構成図である。

【図２０】　従来のマルチメディア情報システムの概略構成図である。

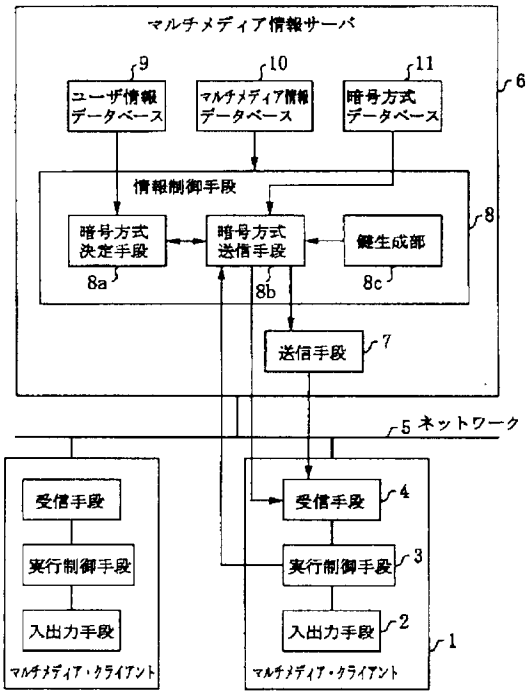
【図２１】　従来のマルチメディア情報システムにおけるメディアデータの構成図である。

【符号の説明】

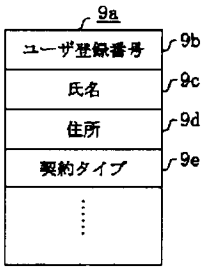
１　マルチメディア・クライアント、２　入出力手段、３　実行制御手段、３ａ　実行情報制御手段、３ｂ　実行手段、４　受信手段、４ａ　復号方式変更手段、４ｂ、４ｃ　復号実行手段、４ｄ　受信制御手段、５　ネットワーク、６マルチメディア情報サーバ、７　送信手段、７ａ　暗号方式変更手段、７ｂ、７ｃ　暗号化実行手段、７ｄ　送信制御手段、８　情報制御手段、８ａ　暗号方式決定手段、８ｂ　暗号方式送信手段、８ｃ　鍵生成部、８ｄ　制御手段、８ｅマルチメディア情報送信手段、８ｆ　実行情報送信方式決定手段、９　ユーザ情報データベース、９ａ　契約情報レコード、９ｂ　ユーザ登録番号、９ｃ　氏名、９ｄ　住所、９ｅ　契約タイプ、９ｆ　マルチメディア情報番号、９ｇ　マルチメデ

ィア実行制御情報、９ｈ　マルチメディア情報番号、９ｉ　マルチメディア実行制御情報、１０　マルチメディア情報データベース、１０ａ　マルチメディア情報レコード、１０ｂ　マルチメディア情報番号、１０ｃ　マルチメディア情報の名称、１０ｄ　実行方式番号、１０ｅ　実行制約条件、１０ｆ　マルチメディア情報、１１　暗号方式データベース、１１ａ　暗号方式レコード、１１ｂ暗号方式番号、１１ｃ　暗号方式の名称、１１ｄ　鍵生成手段、１１ｅ　暗号化手段、１１ｆ　復号手段、１１ｇ　使用可能地域情報、１２　復号手段データベース、１３　暗号化手段データベース、１４　送信データ、１４ａ　暗号方式番号、１４ｂ　暗号化されたマルチメディア情報、１５　実行方式データベース。

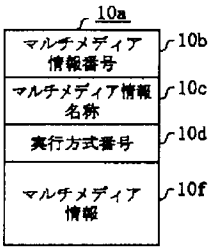
【図１】



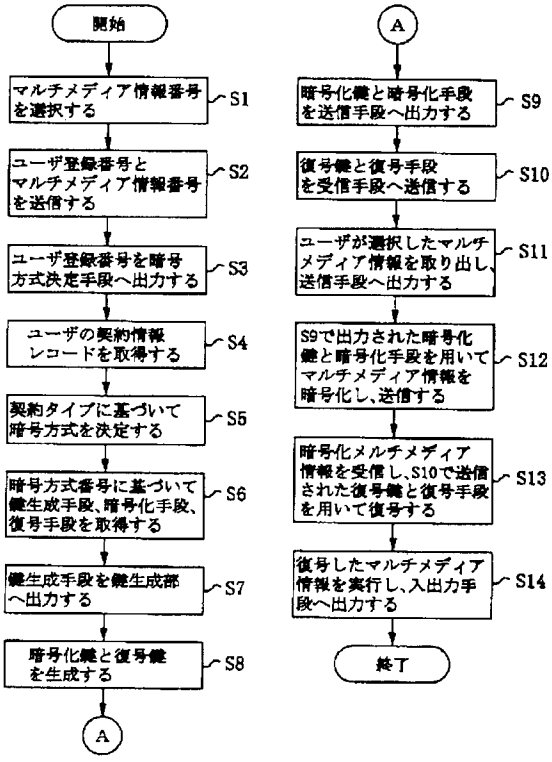
【図２】



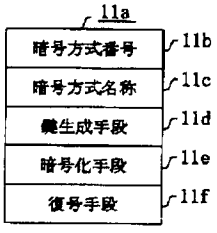
【図３】



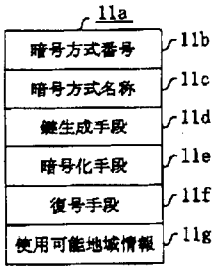
【図５】



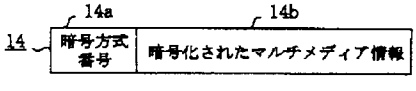
【図４】



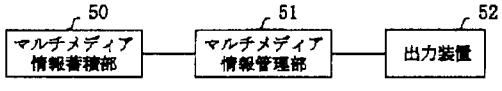
【図９】



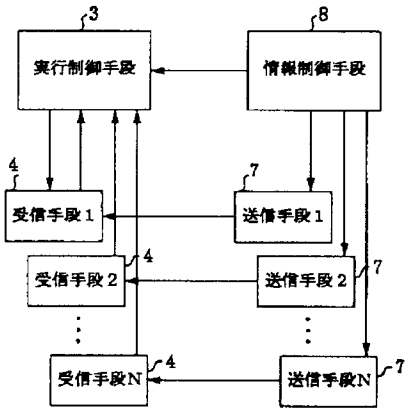
【図１３】



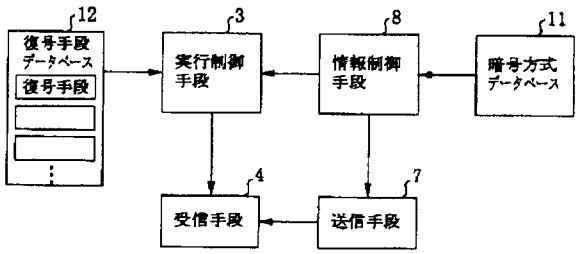
【図２０】



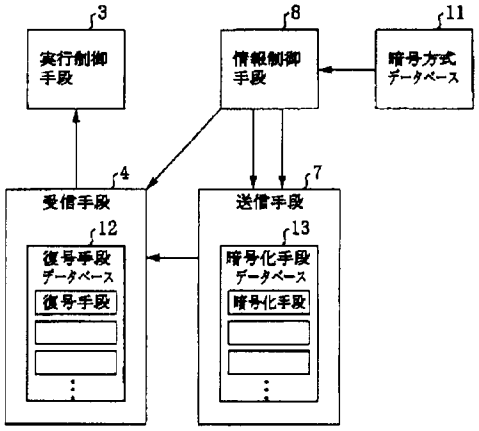
【図６】



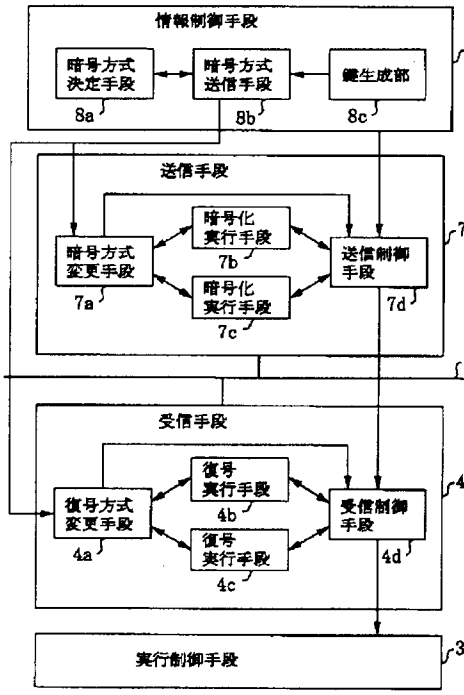
【図７】



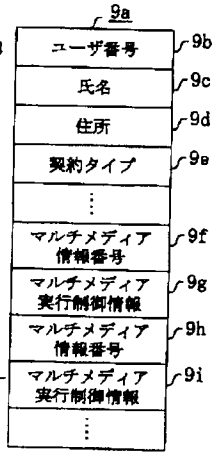
【図８】



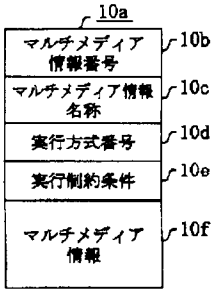
【図１０】



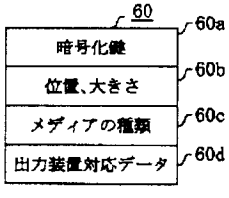
【図１８】



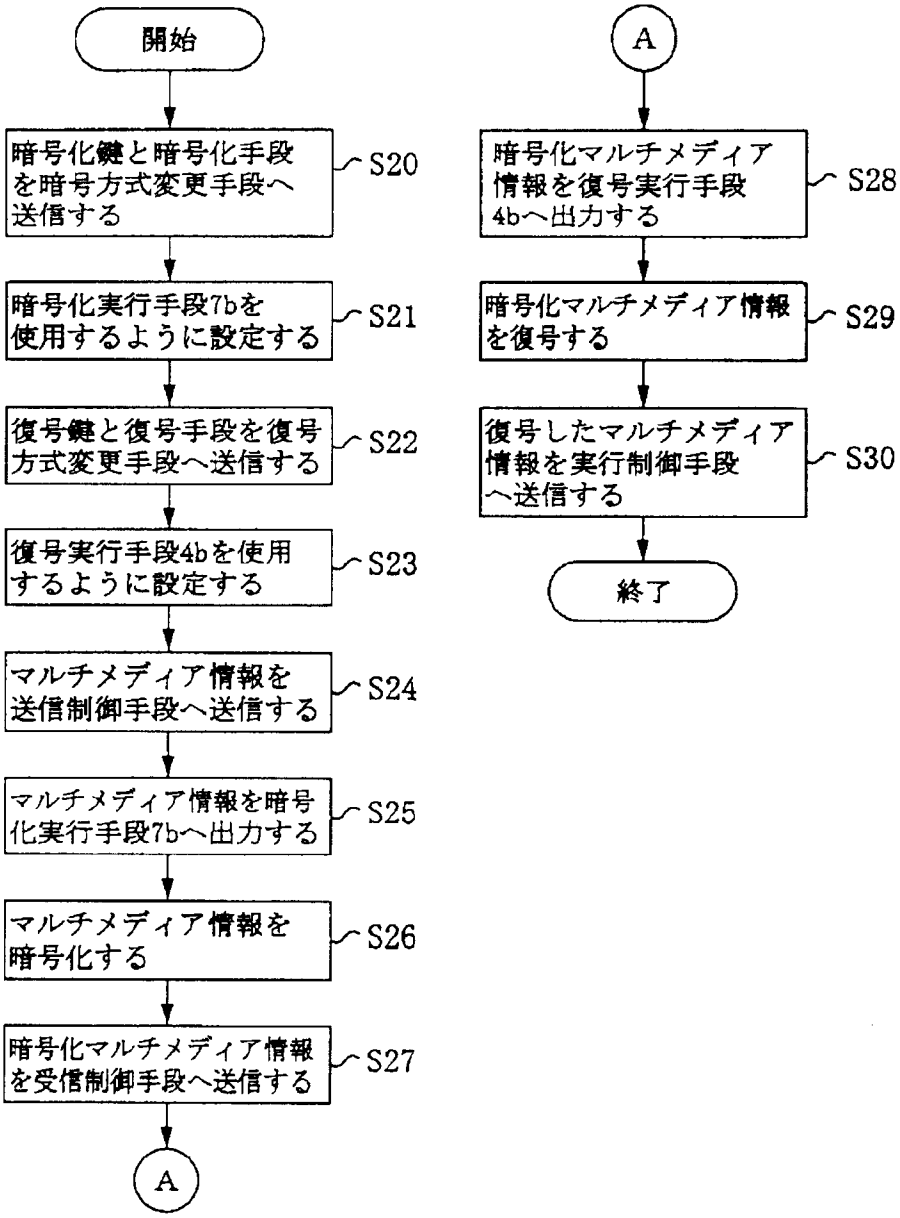
【図１９】



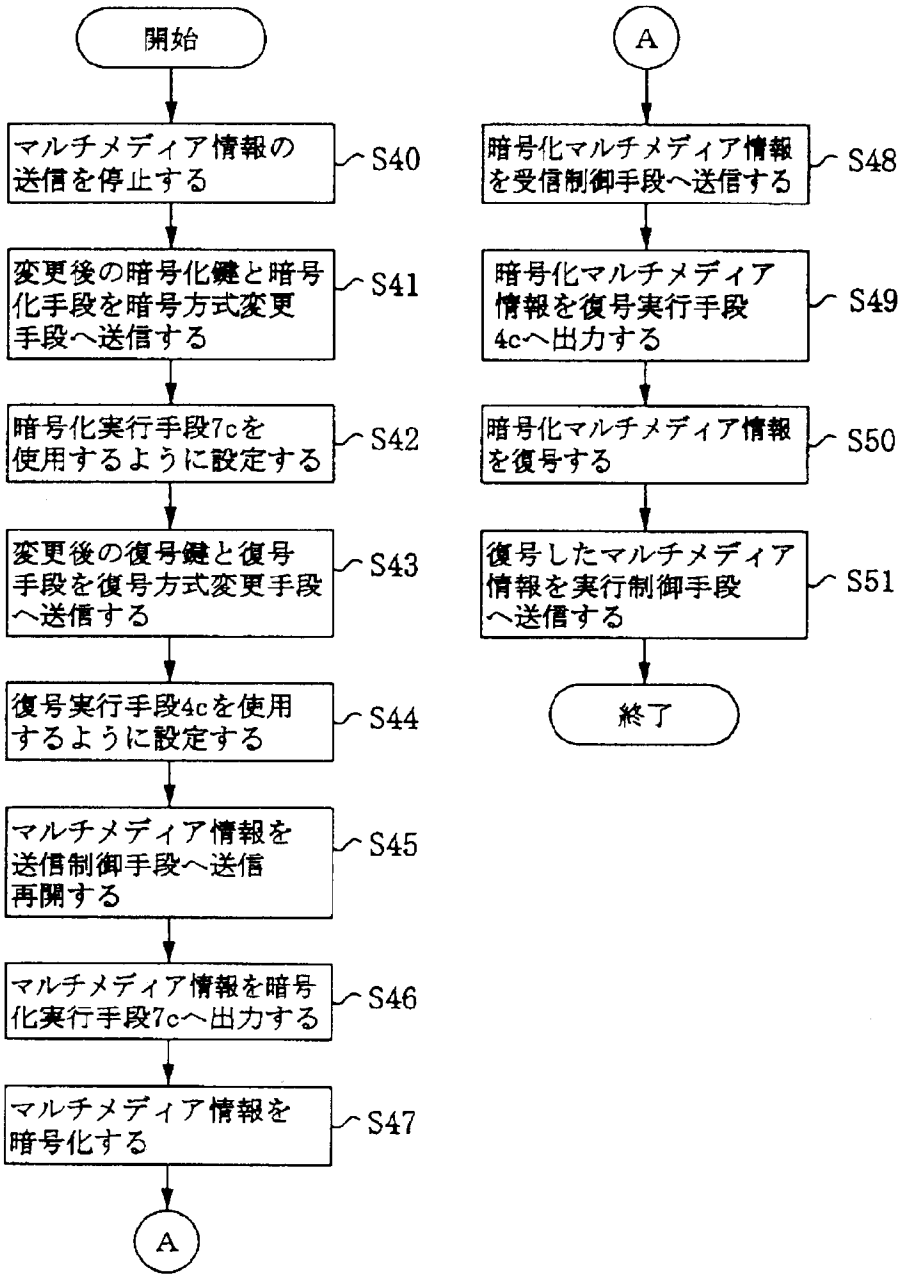
【図２１】



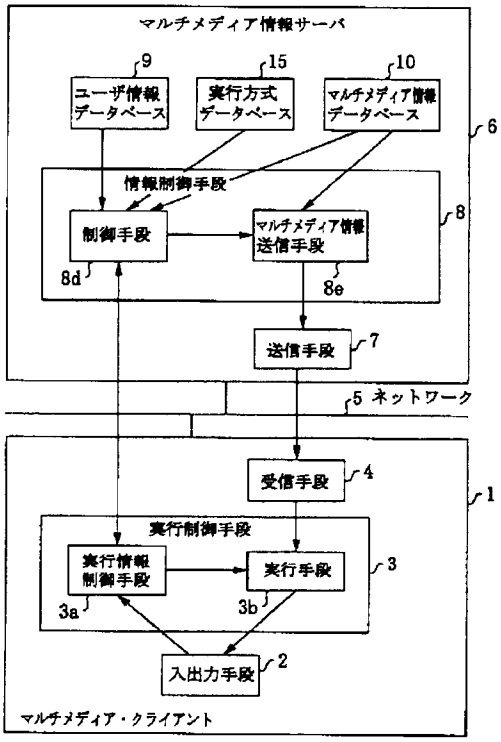
【図１１】


開始
暗号化鍵と暗号化手段を暗号方式変更手段へ送信する
S20
暗号化実行手段7bを使用するように設定する
S21
復号鍵と復号手段を復号方式変更手段へ送信する
S22
復号実行手段4bを使用するように設定する
S23
マルチメディア情報を送信制御手段へ送信する
S24
マルチメディア情報を暗号化実行手段7bへ出力する
S25
マルチメディア情報を暗号化する
S26
暗号化マルチメディア情報を受信制御手段へ送信する
S27
A
A
暗号化マルチメディア情報を復号実行手段4bへ出力する
S28
暗号化マルチメディア情報を復号する
S29
復号したマルチメディア情報を実行制御手段へ送信する
S30
終了

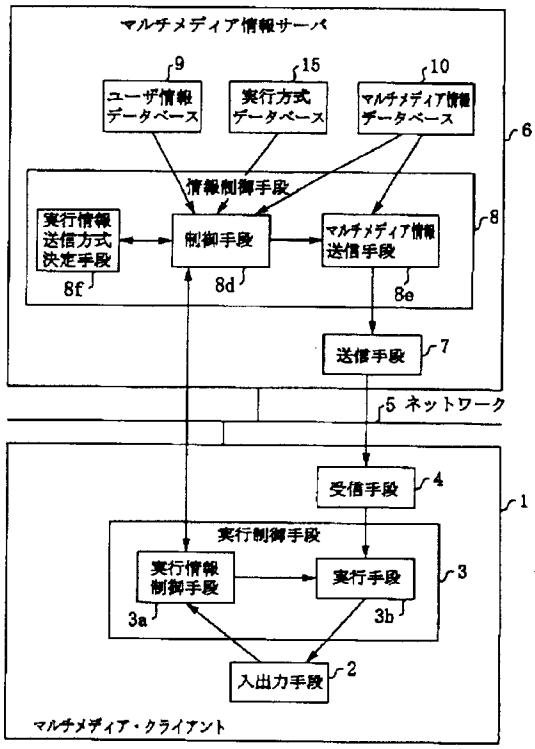
【図１２】


開始
マルチメディア情報の送信を停止する
S40
変更後の暗号化鍵と暗号化手段を暗号方式変更手段へ送信する
S41
暗号化実行手段7cを使用するように設定する
S42
変更後の復号鍵と復号手段を復号方式変更手段へ送信する
S43
復号実行手段4cを使用するように設定する
S44
マルチメディア情報を送信制御手段へ送信再開する
S45
マルチメディア情報を暗号化実行手段7cへ出力する
S46
マルチメディア情報を暗号化する
S47
A
A
暗号化マルチメディア情報を受信制御手段へ送信する
S48
暗号化マルチメディア情報を復号実行手段4cへ出力する
S49
暗号化マルチメディア情報を復号する
S50
復号したマルチメディア情報を実行制御手段へ送信する
S51
終了

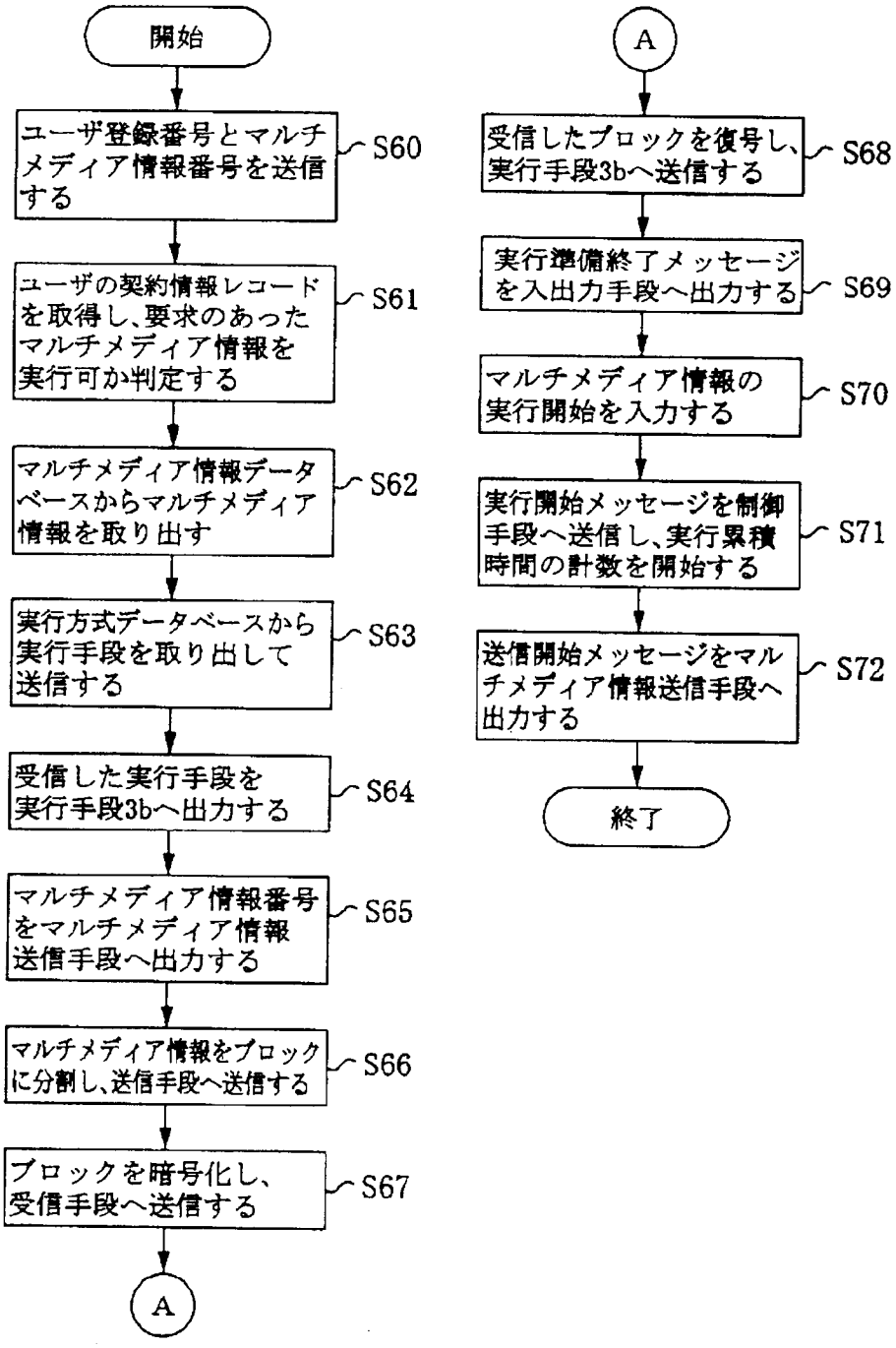
【図１４】


マルチメディア情報サーバ
9
15
10
ユーザ情報データベース
実行方式データベース
マルチメディア情報データベース
6
情報制御手段
制御手段
マルチメディア情報送信手段
8
8d
8e
送信手段
7
5 ネットワーク
受信手段
4
1
実行制御手段
実行情報制御手段
実行手段
3
3a
3b
入出力手段
2
マルチメディア・クライアント

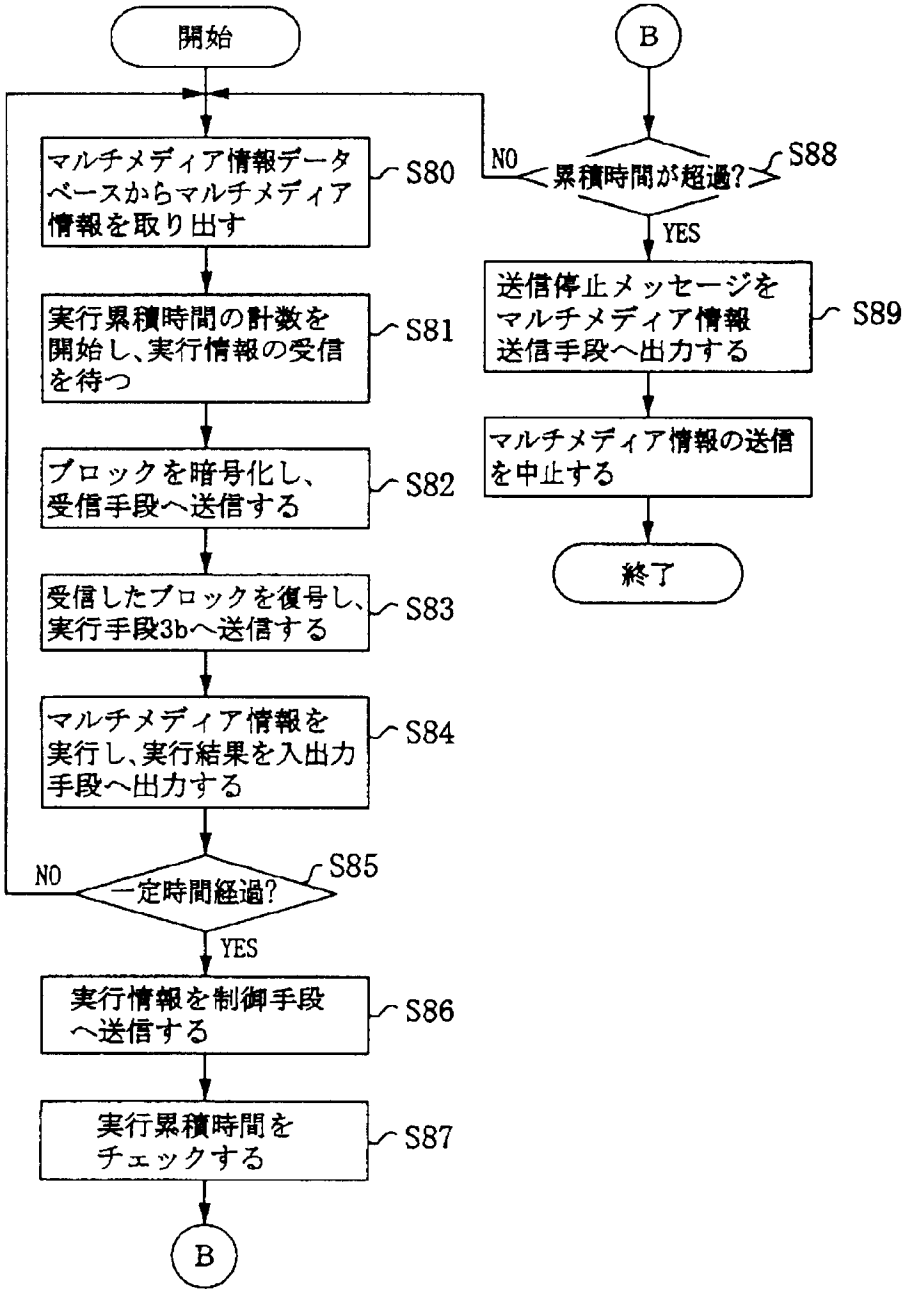
【図１７】


マルチメディア情報サーバ
9
15
10
ユーザ情報データベース
実行方式データベース
マルチメディア情報データベース
6
情報制御手段
実行情報送信方式決定手段
制御手段
マルチメディア情報送信手段
8
8f
8d
8e
送信手段
7
5 ネットワーク
受信手段
4
1
実行制御手段
実行情報制御手段
実行手段
3
3a
3b
入出力手段
2
マルチメディア・クライアント

【図１５】


開始
ユーザ登録番号とマルチメディア情報番号を送信する
S60
ユーザの契約情報レコードを取得し、要求のあったマルチメディア情報を実行可か判定する
S61
マルチメディア情報データベースからマルチメディア情報を取り出す
S62
実行方式データベースから実行手段を取り出して送信する
S63
受信した実行手段を実行手段3bへ出力する
S64
マルチメディア情報番号をマルチメディア情報送信手段へ出力する
S65
マルチメディア情報をブロックに分割し、送信手段へ送信する
S66
ブロックを暗号化し、受信手段へ送信する
S67
A
A
受信したブロックを復号し、実行手段3bへ送信する
S68
実行準備終了メッセージを入出力手段へ出力する
S69
マルチメディア情報の実行開始を入力する
S70
実行開始メッセージを制御手段へ送信し、実行累積時間の計数を開始する
S71
送信開始メッセージをマルチメディア情報送信手段へ出力する
S72
終了

【図１６】


開始
マルチメディア情報データベースからマルチメディア情報を取り出す
S80
実行累積時間の計数を開始し、実行情報の受信を待つ
S81
ブロックを暗号化し、受信手段へ送信する
S82
受信したブロックを復号し、実行手段3bへ送信する
S83
マルチメディア情報を実行し、実行結果を入出力手段へ出力する
S84
NO
一定時間経過?
S85
YES
実行情報を制御手段へ送信する
S86
実行累積時間をチェックする
S87
B
B
NO
累積時間が超過?
S88
YES
送信停止メッセージをマルチメディア情報送信手段へ出力する
S89
マルチメディア情報の送信を中止する
終了